Supreme Court, U.S.
FILED

(1)

No. 02 969 DEC 10 2002

OFFICE OF THE CLERK

In The

Supreme Court of the United States

ROBERT C. KONOP,

Petitioner,

v.

HAWAIIAN AIRLINES, INC.,

Respondent.

On Petition For Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

PETITION FOR WRIT OF CERTIORARI

ROBERT C. KONOP
Petitioner, Pro Se
P.O. Box 5065
Playa del Rey, CA 90293
(310) 305-2837

88 pp

QUESTIONS PRESENTED

A Hawaiian Airlines vice president accessed Petitioner Konop's secure internet communications facility, using a scheme of misrepresentation. As a result of his access, the Hawaiian vice president used the computer in his office to acquire the contents of private electronic communications. Those communications were then used and disclosed to others, supporting efforts by the company to gain ratification of a concessionary labor contract. At the same time, the airline used the pilfered information to oppose Petitioner Konop's efforts to obtain alternative union representation.

Although the Court of Appeals agreed that Konop's secure internet communications were "electronic communications," a majority of the appeals panel concluded that Konop's private internet communications did not enjoy the protections of the *Wiretap Act*. That law prohibits the unauthorized acquisition, disclosure, and use of secure electronic communications.

1. Does the *Wiretap Act* protect secure internet communications, from interception, when those private electronic communications are temporarily maintained in intermediate storage incidental to transmission over the internet?

2. Does a literal application of the *Wiretap Act* impede legitimate law enforcement on the internet?

PARTIES TO THE PROCEEDING

Petitioner

Petitioner is Robert C. Konop, an individual citizen of the United States, residing in the Central District of California. Petitioner has no corporate affiliations. Robert C. Konop was the Plaintiff in the District Court, and the Appellant in the Court of Appeals for the Ninth Circuit.

Respondent

Hawaiian Airlines is a corporation which is publicly traded. Petitioner is unaware of any publicly traded company owning ten percent (10%) or more of the corporation's stock. Respondent Hawaiian Airlines was the Defendant in the District Court, and the Appellee before the Ninth Circuit Court of Appeals.

TABLE OF CONTENTS

	Page
Questions Presented	i
Parties to the Proceeding	ii
Table of Contents	iii
Table of Authorities	v
Opinions Below	1
Statement of Jurisdiction	1
Constitutional and Statutory Provisions Involved	1
Statement of the Case	2
A. Statutory Background	2
B. The Federal Statutory Scheme	3
C. Proceedings Below	6
Reasons for Granting the Petition	9
I. The Ninth Circuit's Revised Opinion Conflicts with the Circuit's Own Precedent and the Literal Terms of the Law	11
II. The Appeals Courts Diverge On The Proper Application and Interpretation of the Electronic Communications Privacy Act	16
III. The Question Presented Is Important to the Consistent and Efficient Operations of the Courts, and in the Public's Interests	21
IV. The Question Presented is Important to the Proper Operation of Law Enforcement	25
Conclusion	30

TABLE OF CONTENTS – Continued

Page

Appendix

Appendix A

Court of Appeals Opinion, 8/24/02: *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) ..... App. 1

Appendix B

Court of Appeals Order Denying Petitions For Rehearing, 10/4/02 ..... App. 46

Appendix C

(Excerpts)

18 U.S.C. § 2511(1) ..... App. 47

18 U.S.C. § 2701(a) ..... App. 47

18 U.S.C. § 2703 ..... App. 48

TABLE OF AUTHORITIES

Page

CASES:

Bartnicki v. Vopper, 532 U.S. 514 (2001) .. 14, 19, 23, 26, 27

Bohach v. City of Reno, 932 F.Supp. 1232 (D. Nev. 1996) 23

Boner v. McDermott, 191 F.3d 463 (D.C. Cir. 1999) 12

Crowley v. Cybersource, Corp., 166 F.Supp. 2d 1263 (N.D. Calif. 2001) 14, 24

Eagle Investment Systems v. Tamm, 146 F.Supp. 2d 105 (D. Mass. 2001) 22

Guest v. Leis, 255 F.3d 325 (6th Cir. 2001) 16, 20

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) ..... *passim*

Konop v. Hawaiian Airlines, Inc., 262 F.3d 972 (9th Cir. 2001) 7

Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001) ..... *passim*

Sorenson v. Secretary of the Treasury, 475 U.S. 851 (1986) 15

Steve Jackson Games v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994) ..... *passim*

Steve Jackson Games v. U.S. Secret Service, 816 F.Supp. 432 (W.D. Tex. 1993), aff'd, 36 F.3d 457 (5th Cir. 1994) 17

Stone v. Caplan, 10 F.3d 285 (5th Cir. 1994) 15

United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992) (en banc) 15

United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990) 24

TABLE OF AUTHORITIES – Continued

Page

United States v. Moriarty, 962 F.Supp. 217 (D. Mass. 1997) 20, 21

United States v. Reyes, 922 F.Supp. 818 (S.D.N.Y. 1996) 23

United States v. Ron Pair Enterprises, Inc., 489 U.S. 235 (1989) 18

United States v. Smith, 155 F.3d 1051 (9th Cir. 1998), cert. denied, 525 U.S. 1071 (1999) ..... *passim*

United States v. Turk, 526 F.2d 654 (5th Cir. 1976), cert. denied, 429 U.S. 823 (1976) 18

Wesley College v. Pitts, 974 F.Supp. 375 (D. Del. 1997), aff'd without opinion, 172 F.3d 861 (3rd Cir. 1998) 23

STATUTES:

The First Amendment, U.S.C.A. First 1, 5, 16

The Fourth Amendment, U.S.C.A. Fourth 2, 5, 16

Omnibus Crime Control and Safe Streets Act of 1968, Pub. Law 90-351, 82 Stat. 212 2

Electronic Communications Privacy Act of 1986, Pub. Law No. 99-508, 100 Stat. 1848 ..... *passim*

Railway Labor Act (45 U.S.C. § 151-188) 41 Stat. 469 (2/28/20); 49 Stat. 1189 ((4/10/36) 6, 7

The USA PATRIOT Act, Pub. Law No. 107-56, 115 Stat. 272 (10/26/01) 18, 27

Stored Communications Act (18 U.S.C. § 2701 et seq.) Pub. Law No. 99-508, 100 Stat. 1848 ..... *passim*

TABLE OF AUTHORITIES – Continued

Page

Wiretap Act (18 U.S.C. § 2510 et seq.), Pub. Law 90-351, 82 Stat. 212 ..... *passim*

18 U.S.C. §§ 2510(4) 5, 13, 18, 22, 24

18 U.S.C. §§ 2510(5) 13, 22, 24

18 U.S.C. §§ 2510(12) 5, 13, 22

18 U.S.C. §§ 2510(17) 22, 24

18 U.S.C. § 2511 ..... 2, 6, 10, 19, 29

18 U.S.C. § 2511(1)(a) 5, 11, 12, 22

18 U.S.C. § 2511(1)(c) 5, 10, 21

18 U.S.C. § 2511(1)(d) 5, 10, 21

18 U.S.C. § 2511(2)(g)(i) 5, 10

18 U.S.C. § 2516 6

18 U.S.C. § 2518 6

18 U.S.C. § 2701 ..... 2, 6, 20

18 U.S.C. § 2701(a) ..... *passim*

18 U.S.C. § 2703 ..... *passim*

18 U.S.C. § 2703(a) 5, 10, 18, 25, 26

18 U.S.C. § 2711 20

28 U.S.C. § 1254(1) 1

28 U.S.C. § 1331 6

28 U.S.C. § 1337 6

28 U.S.C. § 2403(a) 1

45 U.S.C. §§ 151-188 ..... 6, 7

TABLE OF AUTHORITIES – Continued

Page

OTHER AUTHORITIES:

Supreme Court Rule 29.4(b) 1

Senate Rep. No. 90-1097, (1968), reprinted in 1968 U.S.C.C.A.N. 2153 ..... 4, 12, 25

Senate Report 99-541, (1986), reprinted in 1986 U.S.C.C.A.N. 3557 ..... *passim*

Senate Report 106-932 (2000) 6

H.R. Report No. 99-647 (1986) 20, 28

Jarrod J. White, *Commentary, E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 Ala L. Rev. 1079 (1997) 16

Black's Law Dictionary, West Publishing, 1979 29

"Carnivore – Diagnostic Tool" FBI Programs and Initiatives – by Donald M. Kerr, Director Lab Division, Federal Bureau of Investigation from Written testimony before the House Judiciary Committee, subcommittee on the Constitution, 7/24/00 6

PETITION FOR WRIT OF CERTIORARI

Petitioner Konop respectfully petitions that a writ of certiorari issue to review Part I, Section B, of the opinion of the Ninth Circuit Court of Appeals in *Robert C. Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

OPINIONS BELOW

The Ninth Circuit opinion is reported at 302 F.3d 868 (9th Cir. 2002), and is reprinted in the appendix to this petition ("App.") at 1-45. The Ninth Circuit's withdrawn opinion is reported at 236 F.3d 1035 (9th Cir. 2001). The order denying rehearing or the suggestion for a rehearing en banc is unreported and is reprinted at App. 46.

STATEMENT OF JURISDICTION

The judgment and opinion of the Ninth Circuit Court of Appeals was entered on August 23, 2002. Timely petitions for rehearing and for rehearing en banc were denied on October 4, 2002. App. 46. The jurisdiction of this court is invoked pursuant to 28 U.S.C. § 1254(1). In light of the potential applicability of 28 U.S.C. § 2403(a), notification and service has been provided to the U.S. Solicitor General in accordance with Supreme Court Rule 29.4(b).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The First Amendment to the United States Constitution provides in pertinent part that "Congress shall make no law . . . abridging the freedom of speech." In this case, the Ninth Circuit majority's opinion interprets the Electronic Communications Privacy Act as limiting Petitioner Konop's rights to free speech, and his

enjoyment of privacy, in his internet communications.

The Fourth Amendment to the United States Constitution provides in pertinent part that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated." In this case, however, the majority opinion limits the security which Petitioner Konop enjoys in his person and papers, deferring to law enforcement rights which Congress otherwise sought to protect through enactment of the Electronic Communications Privacy Act.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 et seq. ("ECPA"), provides the controlling law. The ECPA states that no person may, without authorization, access a communications facility or obtain the contents of a wire or electronic communication through the use of a device. The pertinent ECPA sections, 18 U.S.C. §§ 2511, 2701, and 2703, are set forth within the Appendix, at App. 47-49.

STATEMENT OF THE CASE

A. Factual Background

Robert C. Konop brought this action against his employer, Hawaiian Airlines. Konop claimed that Hawaiian's officers interfered with the internal union organizational business of its pilots. Without authorization, a Hawaiian vice president accessed Petitioner Konop's secure internet communications facility. Then, in furtherance of Hawaiian's campaign to gain ratification of a concessionary labor contract from its pilots, the airline's

vice president acquired the contents of private electronic communications which opposed ratification of the proposed agreement.

Hawaiian's officer subsequently passed details of the purloined internet communications to the airlines' president. Hawaiian's president, in turn, disclosed the contents of a stolen communication to the head of an opposing union faction. Hawaiian's president claimed that the disclosure was necessary to facilitate ratification of the proposed concessionary union contract, a contract which Konop's faction opposed. In addition, the intercepted electronic communications were used to counter Konop's concerted efforts to seek alternative union representation for Hawaiian's pilots.

Neither Hawaiian's vice president, president, nor the head of the opposing labor faction were authorized user's of Konop's secure communications facility. In any event, the authorized users of Konop's internet communications system were required to agree to access limitations and non-disclosure covenants in order to be granted access authorization. Access was accomplished through the use of a password-protected security system. Hawaiian's officers were specifically prohibited access to Konop's secure internet communications facility.

B. The Federal Statutory Scheme

In 1967 Congress passed the Wiretap Act (18 U.S.C. § 2510 et seq.). This law was adopted in furtherance of the rights defined under the U.S. Constitution, and for the "dual purpose (1) protecting the privacy of wire [electronic] and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire [electronic] and oral communications

may be authorized," Senate Rep. No. 90-1097, at 66 (1968), reprinted in 1968 U.S.C.C.A.N. 2153. Later, Congress also recognized that the absence of wiretap protections "may unnecessarily discourage potential customers from using innovative communications systems," and "may unnecessarily discourage American business from developing new innovative forms of telecommunications and computer technology." Senate Report 99-541, at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3557.

Congress found that "[t]he tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communications is seriously jeopardized." Senate Report 90-1097, supra at 67. More specifically, Congress determined:

> "Commercial and employer-labor espionage is becoming widespread. It is becoming increasingly difficult to conduct business meetings in private. Trade secrets are betrayed. Labor and management plans are revealed. No longer is it possible, in short, for each man to retreat into his home and be left alone. Every spoken word relating to each man's personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor's advantage." [*Id.*]

In 1986, Congress concluded that the development of cellular telephones, computers, and other new means of electronic communication made the problem even worse. "[T]remendous advances in telecommunications and computer technology have carried with them comparable technological advances in surveillance devices and techniques," increasing the risk that communications "may be

open to possible wrongful use and public disclosure." Senate Report 99-541, at 3. It was for that reason, and to assure the protection of individual rights under the First and Fourth Amendments, that Congress passed the Electronic Communications Privacy Act of 1986. Senate Report 99-541, supra at 1.

Using provided definitions, the provisions of the ECPA can be simply and literally applied. Once a communication can be characterized as an *electronic communication*, its contents may not be acquired through the use of a device without proper authorization (18 U.S.C. §§ 2510(4) and (12); § 2511(1)(a)). Using a device for the unauthorized *acquisition* of a communication is an unlawful *intercept* in violation of the *Wiretap Act*. Where a communication service was accessed to obtain a wire or electronic communication, the *Stored Communications Act* was also violated (18 U.S.C. § 2701(a)). Further, the contents of an electronic communication, which has been intercepted without proper authorization, may not be *used* or *disclosed* without committing further violations of the statute (18 U.S.C. §§ 2511(1)(c) and (d)).

Although it is not unlawful to *intercept* an electronic communication which is readily accessible to the general public (18 U.S.C. § 2511(2)(g)(i)), the interception of a private electronic communication is prohibited (18 U.S.C. § 2511(1)(a)). In any event, any governmental entity may require the *disclosure* of a wire or electronic communication, which is maintained in intermediate or backup storage, through the use of a warrant or subpoena (18 U.S.C. § 2703(a)). However, where law enforcement seeks to directly *access* and *intercept* electronic communications, such as with the Justice Department's Carnivore

equipment, a *wiretap order* is required[1] (18 U.S.C. §§ 2516 and 2518).

C. Proceedings Below

Petitioner Konop raised federal questions with respect to Hawaiian's violation of both the *Railway Labor Act* (45 U.S.C. § 151-188) and the *Electronic Communications Privacy Act* (Titles I and II, the *Wiretap Act* and the *Stored Communications Act*) (18 U.S.C. § 2510 et seq.). The U.S. District Court possessed jurisdiction under the terms of 28 U.S.C. §§ 1331 and 1337.

Based upon opposing motions for summary judgment, the District Court granted summary judgment against Petitioner Konop on all claims, except his retaliation claim under the *Railway Labor Act*. On the retaliation claim, the district court entered judgment against Konop following a bench trial. Konop timely appealed the district court's judgment on all claims, except those which had been brought under state tort law.

In Petitioner Konop's appeal to the Ninth Circuit, Konop argued that the provisions of both the Wiretap Act (18 U.S.C. § 2511) and the Stored Communications Act (18 U.S.C. § 2701) were violated by the misconduct of Hawaiian's officers. First, Konop claimed that there were sufficient material issues for trial concerning the Hawaiian vice president's illegal access to a secure communications

---

[1] See: *"Carnivore – Diagnostic Tool"* FBI Programs and Initiatives – written testimony before the House Judiciary Committee, subcommittee on the Constitution, by Donald M. Kerr, Director Lab Division, Federal Bureau of Investigation, 7/24/00, Tr 37-39, referenced within; Senate Report 106-932 (2000), pages 13 and 22.

facility without authorization, and in violation of a specific prohibition against such access. Second, Konop argued that this illegal access, accomplished using a computer in the vice president's office, and using intentional misrepresentations, resulted in Hawaiian acquiring the contents of private electronic communications. Konop also contended that these specific acts of misconduct were prohibited by the non-interference provisions of the Railway Labor Act (45 U.S.C. §§ 151-188).

On January 8, 2001, a Ninth Circuit panel unanimously found in Petitioner Konop's favor. *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001) ("Konop I"). The panel reversed the district court on all issues except a peripheral claim that Konop's trial subpoenas had been improperly quashed. The appeals panel concluded that there were material issues with respect to Hawaiian's violation of both the *Wiretap Act* and the *Stored Communications Act*. This misconduct, the appeals panel reasoned, also created a material issue with respect to Hawaiian's further violation of the *Railway Labor Act*.

Based upon Hawaiian's Petition for Rehearing En Banc, and amicus briefs from both the U.S. Department of Justice and the California District Attorneys Association, on August 28, 2001, with a dissent, the appeals panel withdrew its January 8, 2001 opinion. *Konop v. Hawaiian Airlines, Inc.*, 262 F.3d 972 (9th Cir. 2001). The panel's original opinion had incorporated references to the use of false pretenses, by which Hawaiian gained access to Konop's private communications. The Justice Department and the District Attorneys reasoned that this reference might impede legitimate law enforcement efforts on the internet.

Hawaiian and its amici also argued that the interception of an electronic communication could not occur while such communication was in intermediate, or backup electronic storage, incidental to its transmission. Instead, the law enforcement amici argued, Hawaiian had neither violated the access prohibitions of the *Stored Communications Act*, through its scheme of misrepresentation to gain access to Konop's communication system, nor had Hawaiian violated the *Wiretap Act*, even though Hawaiian had obtained the contents of electronic communications through the use of a device.

On August 23, 2002, the Ninth Circuit's panel issued a new decision, written by Judge Boochever, with a dissent by Judge Reinhardt. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) ("Konop II"). Therein, the panel majority reversed itself with respect to the issue of Hawaiian's violation of the Wiretap Act. The panel unanimously agreed, however, to each of the other elements for which it had originally found in Petitioner Konop's favor.

On September 4, 2002, Konop petitioned the Ninth Circuit's panel for its reconsideration, rehearing, or for a rehearing en banc. Therein, Konop observed that the Ninth Circuit's panel failed to consider both the literal provisions of the Wiretap Act, and ample proof of Congressional intent with respect to the protection of electronic communications. Konop pointed out that contents of electronic communications are subject to interception both while moving in transit and while in intermediate or backup storage incidental to transmission. Further, for law enforcement purposes, stored communications are subject to required disclosure through the use of a warrant or subpoena.

In an October 4, 2002 order, the Ninth Circuit's panel denied Konop's Petition for Rehearing. While the Opinion's author, Judge Boochever, voted to deny rehearing, he recommended that the case be reheard en banc. Judge Reinhardt voted to grant the requested rehearing; however, he voted to deny the rehearing en banc. Judge Paez voted to deny both the requested rehearing and the rehearing en banc.

REASONS FOR GRANTING THE PETITION

Petitioner Konop seeks a writ of certiorari for the Court's review and guidance with respect to Part I, Section B, of the Ninth Circuit's revised opinion. That portion of the opinion reflects the panel majority's failure to properly apply the Wiretap Act to the illegal *intercept*, *disclosure*, and *use* of private electronic communications.

Since its passage, courts have struggled with the application and interpretation of the ECPA. The statute has unique technical definitions and applications. The courts have fumbled with the law much like an ordinary consumer attempting to operate an elaborate home entertainment system with a new universal remote control. There have been missteps and confusion. However, the law itself, as related to the interception of private electronic communications, is not as complex as the Appeals Court suggests.

> "The Fifth Circuit has characterized the Wiretap Act as 'famous (if not infamous) for its lack of clarity.' We have noted that the Fifth Circuit 'might have put the matter too mildly. Indeed, the intersection of the Wiretap Act and the Stored Communications Act is a complex, often convoluted, area of the law.'"

Konop I, supra at 1042, quoting; *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994), and; *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998), cert. denied, 525 U.S. 1071 (1999) (citations omitted).

The *Wiretap Act* and the *Stored Communications Act* ("SCA") make up *Titles I* and *II* of the Electronic Communications Privacy Act. As applied to the present case, the law simply prohibits unauthorized *access* to an electronic communications facility and acquiring the contents of an electronic communication through the use of a device. 18 U.S.C. §§ 2511(1) and 2701(a).

Applying the ECPA literally, the determination of an illegal *intercept* is no more complex than ascertaining two elements. First, an electronic communication must exist. Then, someone must have used "a device" to obtain the contents of the communication without authorization. However, the required *disclosure* of a communication is not an illegal intercept (18 U.S.C. § 2703(a)), nor is obtaining the contents of an electronic communication which is readily accessible to the general public (18 U.S.C. § 2511(2)(g)(i)).

A majority on the Ninth Circuit's panel erroneously concluded additional requirements for an "intercept," beyond those provided by Congress. Those court-added requirements, for a "contemporaneous transmission," not only defeat the privacy protections which Congress specifically provided, but the panel majority also circumvented the law's proscription against the *disclosure* and *use* of electronic communications which have been wrongly acquired (18 U.S.C. § 2511(1)(c) and (d)).

I. The Ninth Circuit's Revised Opinion Conflicts with the Circuit's Own Precedent and the Literal Terms of the Law.

In *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998), cert. denied, 525 U.S. 1071 (1999), a three-judge panel determined that unauthorized *access* to a communications facility was a "lesser included offense of interception," ultimately violating both 18 U.S.C. §§ 2511(1) and 2701(a). *Smith*, supra at 1058. Following this direction, in its original opinion, the panel in this case quoted *Smith* in detail to conclude that Hawaiian's officer violated the terms of both the Wiretap Act (18 U.S.C. § 2511(1)(a)) and the Stored Communications Act (18 U.S.C. § 2701(a)). *Konop I*, supra 1044-46.

> "The word *intercept* entails actually acquiring the contents of a communication, whereas the word *access* merely involves being in a position to acquire the contents of a communication. In other words, *access* is, for all intents and purposes, a lesser included offense (or tort, as the case may be) of *interception*."

U.S. v. Smith, supra at 1058.

According to the Ninth Circuit's original analysis, statutory violations occurred when Hawaiian's vice president first accessed Petitioner Konop's secure internet website, then obtained the contents of Konop's private electronic communications through the use of a device. *Konop I*, supra at 1048. The unauthorized access of the communications facility was a necessary first step in the ultimate *interception*, then in the proscribed *use* and *disclosure* of the communications. *Smith*, supra at 1058. The result was consistent with the literal terms of the law, its definitions, and the Ninth Circuit's precedent.

Based upon the concerns of Hawaiian's law enforcement amici, a majority of the Ninth Circuit's panel then reversed itself. The panel majority now holds that the unauthorized access of a communications facility still violates the SCA. However, under the panel majority's revised opinion, even when that trespass uses a device to obtain the contents of electronic communications, the added *use* and/or *disclosure* of those private communications is simply a part of the original trespass, which the majority now holds are otherwise unprotected. This result is wrong.

The majority's revised opinion is inconsistent with the literal terms of the law and the stated intent of Congress. "[P]rohibiting disclosure furthers the freedom of speech, and reduces the damage caused by unlawful eavesdropping." *Boner v. McDermott*, 191 F.3d 463, 478 (D.C. Cir. 1999) (The provisions of the Wiretap Act, prohibiting the *disclosure* of intercepted communications, support free speech). "To assure the privacy of oral [electronic] and wire communications, [the Wiretap Act] *prohibits all* wiretapping and *electronic surveillance* by persons other than duly authorized law enforcement officers engaged in the investigation or prevention of specified types of crimes." Senate Report No. 1097, page 66, 90th Congress, 2nd Session, April 29, 1968 (emphasis added).

The Wiretap Act is unequivocal with respect to the elements constituting an *intercept* in violation of the law (§ 2511(1)(a)).

> "*[I]ntercept* means the aural or other acquisition of the contents of any wire, electronic, or oral

> communication through the use of any electronic, mechanical, or other device."[2]

18 U.S.C. § 2510(4).

Assuming that an individual is not an authorized recipient of an electronic communication, as applies here, there is simply a single additional element necessary to constitute an *intercept* in violation of the Wiretap Act. An *electronic communication* must actually exist in order for its contents to be illegally obtained through the "use of a device."

> "*[E]lectronic communication* means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce * * * ."

18 U.S.C. § 2510(12).

The Ninth Circuit's panel was unanimous, concluding that Petitioner Konop's secure website constituted an *electronic communication*. *Konop II*, supra at 876 (App. 11). The Stored Communications Act explicitly provides that an electronic communication continues to exist while it is maintained in intermediate, or backup, storage incidental to its transmission. 18 U.S.C. § 2701(a). A secure internet website exists in intermediate storage incidental to its transmission, and is thus an *electronic communication*. *Konop II*, supra at 875 (App. 8).

---

[2] The term *device* specifically excludes the telecommunications equipment normally used by a communications service, or end user, for the reception of communications. 18 U.S.C. § 2510(5).

Unfortunately, the panel majority's logic hiccuped with respect to the *interception* of an electronic communication.

> "Standing alone, this definition would seem to suggest that an individual 'intercepts' an electronic communication merely by 'acquiring' its contents, regardless of when or under what circumstances the acquisition occurs."

Konop II, supra at 876 (App. 11).

The majority's premise was incorrect. Circumstances are integral to determining an "intercept," and a resultant violation of the statute. First, an electronic communication must exist, then its contents must be obtained through the use of a device. See: *Crowley v. Cybersource, Corp.*, 166 F.Supp. 2d 1263, 1269 (N.D. Calif. 2001). (For an illegal intercept, "there must be a communication and, second, that there be an acquisition of that communication by an 'electronic, mechanical, or other device.'"). Merely obtaining the contents of a communication is not an intercept without the requisite circumstances.

By contrast, the required *disclosure* of an electronic communication, under the terms of 18 U.S.C. § 2703, is not an interception. Both situations might result in obtaining the contents of an electronic communication. However, an individual does not *intercept* an electronic communication merely by obtaining its contents. A violation of the Wiretap Act is entirely dependent upon the circumstances which are present. The panel majority failed to recognize that an electronic communication might be obtained through either an *interception* or a *disclosure*. Cf. *Bartnicki v. Vopper*, 532 U.S. 514, 526-527, 540, and 543 (2001) (The *disclosure* of a wire communication is an act which is separate and distinguishable from an illegal *intercept*).

Once the panel determined that Konop's secure website existed as an *electronic communication*, the specific provisions of the statute determined what constituted an interception in violation of the Wiretap Act. *Stone v. Caplan*, 10 F.3d 285, 289 (5th Cir. 1994) (The goal of statutory construction is to ascertain legislative intent through the plain language of a statute). However, the panel majority erroneously added a contemporaneity requirement, for an *interception* in violation of the Wiretap Act, which does not otherwise exist for an electronic communication. *U.S. v. Koyomejian*, 970 F.2d 536, 541 (9th Cir. 1992) (en banc) (A Court is charged with the duty to interpret the laws as they exist rather than to mold them into a new form meeting its own notion of symmetry).

> "As a general rule, a communication is an electronic communication protected by the wiretap law if it is not carried by sound waves and cannot be fairly characterized as containing the human voice. * * * This term also includes electronic mail, digitized transmissions, and video teleconferences."

Senate Report Number 99-541 at 14, 99th Congress, 2nd Session (1986), reprinted in 1986 U.S.C.C.A.N. 3555.

The dissent notes the inconsistency of the new majority view. The majority's revised opinion wrongly eliminates protections which Congress otherwise provided.

> "To read a contemporaneity requirement into the definition of intercept renders the prohibition against the electronic communication interception largely superfluous, and violates the precept against interpreting one provision of a statute to negate another. (citing, *Sorenson v. Secretary of the Treasury*, 475 U.S. 851 (1986)). * * * If intercept is defined as solely contemporaneous acquisition, then in contravention of

> Congressional intent, at most all acquisitions of the contents of electronic communications would escape the interception prohibition entirely. (citing, Jarrod J. White, Commentary, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 Ala L. Rev. 1079, 1083 (1997))."

Konop II, dissent, supra at 888 (App. 35-36) (internal citations omitted).

There is no logical way to reconcile the panel's revised opinion with the Ninth Circuit's conclusion in *Smith* (supra). More problematical, however, is the inconsistency which the panel majority now reads into the law itself. The majority opinion effectively invalidates specific protections which Congress provided against the wrongful *interception*, *disclosure*, and *use* of private electronic communications. Thus, there exists a matter of important federal law which has not yet been, but should be, settled by the Court.

II. The Appeals Courts Diverge On the Proper Application and Interpretation of the Electronic Communications Privacy Act.

There is a divergence of opinion between the Fifth, Sixth, and Ninth Circuits, concerning the proper interpretation and application of the ECPA. In fact, the Ninth Circuit now possesses two separate views (*ante*). The other Circuits have adopted a number of variations. However, the Sixth Circuit's application is the most draconian, entirely ignoring the protections which Congress specifically anticipated for electronic communications, raising serious First and Fourth Amendment issues. See: *Guest v. Leis*, 255 F.3d 325, 339-40 and Note 7 (6th Cir. 2001)

(Preventing authorized and legal access to a communications facility, and the destruction or alteration of stored communications, is excused by the issuance of a search warrant). Cf. *Steve Jackson Games v. U.S. Secret Service*, 816 F.Supp. 432, 442 (W.D. Tex. 1993), aff'd, 36 F.3d 457, 463 (5th Cir. 1994) (The government's search of a communications facility, which destroyed undelivered e-mails, violated 18 U.S.C. § 2701(a)).

The Fifth Circuit's conclusion that a "contemporaneity" requirement exists, for the interception of an electronic communication, directly conflicts with the Ninth Circuit's conclusion that an *intercept* may also occur while a communication is in intermediate electronic storage incidental to its transmission. *Smith*, supra at 1058 (Access to a communications facility is a lesser included offense of interception). The Fifth Circuit's approach equivocates important public interests in free speech and privacy. *Steve Jackson Games*, supra 463 and Footnote 8 (Interception of an electronic communication requires acquisition contemporaneous with transmission).

An irreconcilable conflict has thus arisen between the Circuits in that unauthorized *access* to a communications facility significantly differs from the illegal *intercept* of an electronic communication.

> "The word *intercept* entails actually acquiring the contents of a communication, whereas the word *access* merely involves being in a position to acquire the contents of a communication."

U.S. v. Smith, supra at 1058.

There is no meaningful difference between a wire communication and an electronic communication while either is in intermediate electronic storage. However, prior to the passage of the USA PATRIOT Act of 2001, the ECPA

(18 U.S.C. § 2703(a)) contained no mechanism for the required *disclosure* of a stored *wire communication* through the use of a warrant or subpoena. Pub. Law No. 107-56, § 209, 115 Stat. 272, 283 (enacted October 26, 2001).

Prior to this, the SCA incorporated a *disclosure* provision only for electronic communications. Thus, Congress previously provided that stored electronic communications possessed a lesser degree of privacy, where its *disclosure* could be required through the use of a warrant or subpoena. The 2001 amendment conformed the *disclosure* requirements for wire communications to those provided for electronic communications.

The USA PATRIOT Act, however, left the definition of an *intercept* entirely intact. It remains the acquisition of a communication through the "use of a device." 18 U.S.C. § 2510(4). It is the application of this provision where the Circuit's diverge. In *U.S. v. Smith*, the Ninth Circuit's panel applied the definition of *intercept* exactly as Congress provided it. In *Steve Jackson Games*, on the other hand, the Fifth Circuit constructively applied a requirement that an *intercept* occurs only contemporaneously with the transmission of an electronic communication. The panel majority in this case adopted the Fifth Circuit's approach. *Konop II*, supra at 879 (App 16). However, the Court has repeatedly emphasized that where a statute's language is plain, "the sole function of the courts is to enforce it according to its terms." *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989) (citations omitted).

The Fifth Circuit's construction was based on its own conclusions in *U.S. v. Turk*, 526 F.2d 654 (5th Cir. 1976), cert. denied, 429 U.S. 823 (1976). Although the Fifth

Circuit's result in *Steve Jackson Games* was entirely correct, the reasoning was flawed. The Fifth Circuit equated two provisions which targeted entirely different conduct. It was this flaw which the Ninth Circuit's majority, in their revised opinion, relied upon in its tacit rejection of the Ninth Circuit's own precedent in *U.S. v. Smith* (supra). *Konop II*, supra at 878-9 (App. 14-15).

In *Steve Jackson*, the Fifth Circuit read the terms *intercept* and *access* as analogous. The Fifth Circuit began with the mistaken premise that § 2703 and § 2511 are directly comparable. *Steve Jackson Games*, supra at 463. However, the *disclosure* of third party communications (§ 2703) is significantly different from directly acquiring the contents of those communications through "the use of a device" (§ 2511). Illegal *access* need not involve acquiring communication contents. *U.S. v. Smith*, supra at 1058. Further, the receipt of an electronic communication, which has been *disclosed,* is entirely different from actually acquiring communication contents through an *intercept*. Cf. *Bartnicki v. Vopper*, supra at 526-527, 540, and 543.

> "The majority's interpretation of the Wiretap Act depends in part on a tortured reading of the Stored Communications Act under which 'access to' a communication is equated with 'acquisition of' a communication, contrary to the clear statutory language."

Konop II, dissent, supra 889 (App. 37).

In *U.S. v. Smith*, the Ninth Circuit seemingly put the issue of overlap between ECPA Title I and Title II to rest (Wiretap Act and Stored Communications Act). There, the *Smith* panel noted that Title II's prohibition against unauthorized *access* to a communication facility would be violated by making unauthorized use of a password and "roaming about" a voicemail system without intercepting

message "contents." *Smith*, supra at 1058. The unauthorized access is prohibited where it alternately results in altering communications, preventing authorized access to the facility, or where an intended recipient of communications was prevented from obtaining them. H.R. Report No. 99-647, at 62-63, (1986). Cf. *Guest v. Leis*, supra 339-40 (The Sixth Circuit rejected the Fifth Circuit's affirmation of an SCA violation by the Secret Service in *Steve Jackson Games*).

Taking the next step, in *Smith,* the Ninth Circuit reasoned that once a message was "retrieved and recorded," the line between Title II and Title I had been crossed, and an "interception" occurred. *Smith*, supra at 1058. The panel's original unanimous opinion, in this case, properly reflected this overlap and the Ninth Circuit's prior reasoning. *Konop I*, supra 1044-46. In fact, the government itself has used identical reasoning to that within the Ninth Circuit's original opinion, and as was specified in *Smith* (supra). In *United States v. Moriarty*, the government distinguished "interception" and "access" by arguing that ECPA Title II "only requires access which, by implication, does not necessitate the acquisition of the communication." 962 F.Supp. 217, 219 (D. Mass. 1997) (Unauthorized access to a communications system, to obtain stored voicemail messages, is prohibited by 18 U.S.C. § 2701).

The ECPA, in fact, has three terms which various courts have erroneously used as synonyms. The words *access*, *intercept*, and *disclosure* are at the core of most misunderstandings with respect to the proper application of the Wiretap Act to stored electronic communications. Where the Wiretap Act and the SCA share the definition of *intercept* (18 U.S.C. § 2711), in its revised opinion, the

panel majority wrongly equates an *intercept* of a communication with *access* to a communications system.

The panel majority ignored the Ninth Circuit's precedent in *U.S. v. Smith*. The panel majority further contravened the intent of Congress to protect private electronic communications from prying eyes, and from the subsequent *use* and *disclosure* of those otherwise private communications. 18 U.S.C. §§ 2511(1)(c) and (d). As expressed by Congress, substantial governmental and public interests are at stake. Judge Reinhardt's dissent further demonstrates that the approach taken by the majority contravenes those important purposes. Therefore, the intervention of the Court is required to exercise its supervisory power and provide needed direction to assure a uniform and effective application of the law by the courts in accordance with the Congressional intent.

III. The Question Presented is Important to the Consistent and Efficient Operation of the Courts, and in the Public's Interests.

A string of district court cases has adopted the erroneous premise and reasoning first set forth in *Steve Jackson Games* (supra).[3] The district courts have generally failed to examine the literal terms of the ECPA, and the fact that the terms *access*, *intercept*, and *disclosure* each describe significantly different conduct. This improper usage has equivocated the purposes and effectiveness of the ECPA with respect to the protection of privacy and free speech on

[3] The magistrate's recommendation in *U.S. v. Moriarty*, supra at 222, is typical of efforts to apply a contemporaneity requirement to the Wiretap Act (§ 2511(1)).

the internet. It has also caused confusion with respect to the methodologies required for effective and proper law enforcement.

In *Eagle Investments,* the district court erroneously used *access* interchangeably with *intercept,* or *acquisition.* In doing this, the district court commented on the original opinion in this case.

> "The Ninth Circuit held that the airline's conduct constituted an unlawful *interception* under the amended Wiretap Act, even though the airline vice president did not *access* the secure information during transmission."

Eagle Investment Systems v. Tamm, 146 F.Supp. 2d 105, 112 (D. Mass. 2001). (emphasis added) (Plaintiff failed to provide evidence that an *intercept* of an electronic communication occurred, or that a device was used to acquire the contents of the communication).

Based upon the facts, the ultimate conclusion in *Eagle Investments* is correct. *Eagle*, supra at 113. There were no circumstances constituting the interception of an electronic communication, or even a claim that the acquired information existed as an electronic communication when it was obtained. 18 U.S.C. §§ 2510(4), (5), (12), (17); 2511(1)(a), and; 2701(a). The plaintiff simply complained that a copy of communication contents had been acquired, the source and circumstances of which were unknown.[4]

---

[4] Copies of these contents might have been purloined from the files of the *originator's computer*, the ultimate recipient's computer, or from a paper file. In any of these circumstances, the data would not constitute an *electronic communication*. An *electronic communication* only exists during the *transfer process*, or while the data is in intermediate or backup storage incidental to its transmission. 18 U.S.C. §§ 2510(12) and 2701(a).

Substantial confusion exists between the proper use of the terms *access* and *intercept*. There have been few cases without some misuse or misapplication of the terminology. However, the Court's recent comments, with respect to the differentiation of a *disclosure* from an *intercept*, should go a long way toward clarifying a portion of the prior confusion. See: *Bartnicki v. Vopper*, supra at 526-527, 540, and 543. Unfortunately, confusion remains.

Most district courts believe that *access* and *acquisition* are synonyms. This approach invalidates the major privacy protections of the ECPA, as the panel majority's revised opinion has done in this case. See: *Wesley College v. Pitts*, 974 F.Supp. 375, 386 (D. Del. 1997), aff'd without opinion, 172 F.3d 861 (3rd Cir. 1998) (Acquisition of the contents of "electronic communications unlawful under the Wiretap Act only if they occur contemporaneously with their transmissions."); *United States v. Reyes*, 922 F.Supp. 818, 836 (S.D.N.Y. 1996) ("Taken together, the definitions thus imply a requirement that the acquisition of [electronic communications] be simultaneous with the original transmission of data."); *Bohach v. City of Reno*, 932 F.Supp. 1232, 1236-37 (D. Nev. 1996) (requiring acquisition during transmission).

> "As a general rule, a communication is an electronic communication protected by the wiretap law if it is not carried by sound waves and cannot be fairly characterized as containing the human voice."

Senate Report Number 99-541, supra at 14.

There are a few examples where district courts have faithfully applied the terms supplied within the ECPA. In *Crowley v. Cybersource*, a Plaintiff sought to invoke the Wiretap Act against the recipient of an e-mail for its illegal interception, disclosure, and use. 166 F.Supp. 2d 1263, 1269 (N.D.Cal 2001) (A communication was not obtained in violation of the Wiretap Act where no device was used to obtain its contents). The district court noted that the contents of communications were not obtained during the transfer process, including during the time in which the electronic communication was in intermediate storage incidental to its transmission.

In *United States v. Meriwether*, the retrieval of data from a pager was properly deemed not to be the interception of an electronic communication. 917 F.2d 955 (6th Cir. 1990) (The examination of data left on a pager, after its receipt by the recipient, does not constitute either intermediate storage or acquisition of the communication through the use of a device). This was a proper and correct use of the terms, definitions, and purposes of the ECPA. 18 U.S.C. §§ 2510(4), (5), and (17); 2511(1).

Although, in *U.S. v. Smith,* the Ninth Circuit attempted to rationalize its split with the Fifth Circuit's analysis in *Steve Jackson Games*, the approaches taken by the two circuits are irreconcilable. The conflict has become even more detrimental to the purposes and protections of the law with the new majority opinion in *Konop II*. The new opinion ignores an exact situation Congress cited where a private electronic communication was protected under the Wiretap Act. Congress specifically recognized the "abuse of electronic surveillance" in "employer-labor espionage." Prior to passage of the Wiretap Act, the Senate noted that the "present state of the law is extremely

unsatisfactory" with respect to the interception of electronic communications, including where "[l]abor and management plans are revealed," as in this case. Senate Report 90-1097, supra at 67.

The split between the Circuits is exacerbated where the result in *Steve Jackson Games* was correct, while the most recent amendment to the ECPA would now require a different result in *U.S. v. Smith*. This situation only adds to the convolutions and complexities which both the Ninth Circuit and Fifth Circuit have lamented. *U.S. v. Smith*, supra at 1055, quoting; *Steve Jackson Games*, supra at 462.

The public and governmental interests are substantial. This is especially true where Congress recognized that the absence of wiretap protections "may unnecessarily discourage potential customers from using innovative communications systems," and "may unnecessarily discourage American business from developing new innovative forms of telecommunications and computer technology." Senate Report 99-541, supra at 5. However, the Court can now readily provide necessary guidance on this important and quickly evolving law of the internet and worldwide electronic communications.

IV. The Question Presented is Important to the Proper Operation of Law Enforcement.

The Ninth Circuit panel withdrew its original opinion based upon concerns expressed by law enforcement. The panel majority noted its trepidation, and change of heart, in its revised opinion.

> "Section 2703(a) of the SCA details the procedures law enforcement must follow to access the contents of stored electronic communications, but

> these procedures are considerably less burdensome and less restrictive than those required to obtain a wiretap order under the Wiretap Act. (citation omitted). Thus, if Konop's position were correct and acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result."

Konop II, supra at 879 (App. 16).

Congress, in fact, *did not* intend the result which the panel majority erroneously attributed to Petitioner Konop. The panel majority's erroneous conclusion was based on intermixing the terms *access* and *intercept*. However, the panel's reference to "Section 2703(a)" does not deal with "access" at all. There, the revised majority opinion erroneously equated the terms *access* and *disclosure*.

This misunderstanding occurred nearly a year after the Supreme Court's discussion of the difference between a *disclosure* and an *intercept,* as prohibited by the Wiretap Act. Cf. *Bartnicki v. Vopper*, supra. The panel majority's error also occurred nearly a year after Congress incorporated a heading change to clarify the fact that ECPA § 2703 deals with the *disclosure* of communications rather than *access* to a communications facility, or the *interception* of electronic communications.

The prior heading of § 2703 caused confusion, by using the word *access* when the section dealt exclusively with the *disclosure* of electronic communications. Thus, Congress changed the heading to better reflect its contents. The heading was changed to "*Required disclosure of*

customer communications or records." Pub. Law No. 107-56, supra § 212 (emphasis added). As would apply to this case, or the concerns expressed by the majority of the Ninth's Circuit's panel, the substance of the section was unchanged.

In *Bartnicki v. Vopper* (supra), each of the three opinions of the Court expressed a clear understanding of the difference between a *disclosure* and an *intercept*, as is described within the ECPA. In spite of that differentiation, however, the lower courts have a less than full understanding that a *disclosure* is entirely different from an *intercept* or to the *access* to a communications facility. Unfortunately, the law enforcement amicus briefs, offered for the Ninth Circuit's reconsideration, entirely misconstrued these important differences.

In their amicus brief, the California District Attorney's Association (CDAA) misread the *disclosure* provisions of ECPA Title II (§ 2703) as involving allowances for *access* rather than for *disclosure*. *CDAA Amicus Brief* at 7-8. At the same time, the amicus brief of the Department of Justice (DOJ) properly read § 2703 as a method for law enforcement to "obtain electronic communications in 'electronic storage.'" However, the DOJ overreacted, assuming that the original opinion (*Konop I*) had imposed an unstated requirement for law enforcement to obtain a wiretap order any time they sought *disclosure* of the contents of electronic communications under § 2703. *DOJ Amicus Brief* at 11-13.

The DOJ pushed the panic button even after recognizing that an *intercept* is qualitatively different from a *disclosure*. The law enforcement amici did not see the bright line distinction between the two terms, where both methodologies ultimately result in obtaining the contents

of electronic communications. The DOJ feared that obtaining the contents of stored electronic communications might be subject to the same non-disclosure protections enforced for wire communications in *U.S. v. Smith* (supra). However, prior to the USA PATRIOT Act, the disclosure of a wire communication, in intermediate storage, could not be compelled by a warrant or subpoena, as used by the SEC in *Smith*. The House Report on this provision provided an example which was the exact basis for the Ninth Circuit's conclusion in *Smith*.

> "The contents of the voice portion of a wire communication in storage such as with 'voice mail' may not be obtained under this section."

House Report 99-647, supra at 67. (Examining the limits of a search warrant or subpoena issued under § 2703).

Rather than building on correct reasoning in *U.S. v. Smith*, the panel's revised opinion (*Konop II*) had its roots in the faulty premise espoused in *Steve Jackson Games* (supra). The Fifth Circuit wrongly surmised that *access* and *intercept* are analogous. This misunderstanding was compounded by the hysterics of Hawaiian's attorney, who claimed that the Appeals Court's original analysis would potentially brand millions of private citizens, investigators, and law enforcement officers "as felons." This, Hawaiian's attorney erroneously claimed, would result simply because they "may have occasion to access information on websites." Hawaiian's *Petition For Rehearing En Banc*, page 15, dated 1/29/01. However, Hawaiian's conjecture is unsupported by the law.

> "This provision addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public. * * * This subsection does

> not prevent broad authorizations to the general public to access such a facility."

Senate Report 99-541, supra at 35-36. (Discussing the protection against unauthorized access to a communications facility under § 2701(a)).

At the same time, Hawaiian's law enforcement amici interpreted the unanimous original decision (*Konop I*) as proscribing the use of false pretenses in the furtherance of legitimate law enforcement. The law enforcement amici read a single reference, to the misrepresentations of Hawaiian's officer, as barring legitimate misrepresentations by law enforcement officers in pursuit of criminal evidence. *DOJ Amicus Brief* at 16. This conclusion was also wrong and unsupported by the law, or by any reasonable application of the original decision in *Konop I* (supra).

The law enforcement amici wrongly read misrepresentations, constituting nothing less than wire fraud, as barring their own misrepresentations in the pursuit of legitimate criminal evidence. However, the original unanimous opinion of the Ninth Circuit, in this case, simply failed to mention the involved *scienter*, or Hawaiian's "guilty knowledge" in the efforts of its vice president "to deceive or manipulate" for some wrongful purpose. *Black's Law Dictionary*, West Publishing, 1979. This ill-motive would certainly not be present in any legitimate law enforcement activity. The distinction between the two types of misrepresentation was not discussed in *Konop I* (supra).

There is a significant difference between *access* to a communications facility (§ 2701), *interception* of an electronic communication (§ 2511), and the requirement for the *disclosure* of a wire or electronic communications through the use of a warrant or a subpoena (§ 2703).

> "Subsection (a) of section 2703 provides requirements for government to obtain the contents of an electronic [or wire] communication * * * in electronic storage * * * ."

Senate Report 99-541, supra at 38.

The panel majority was misguided when it withdrew and reissued its opinion in an effort to aide law enforcement on the internet. The majority misread the literal terms of the law. The Ninth Circuit's panel also wrongly ignored the substantial government interest, expressed by Congress, for the protection of privacy and free speech. The means for law enforcement to seek *access* to communications facilities, require the *disclosure* of stored communications, or *intercept* electronic communications, are readily accomplished through the means which Congress provided. Thus, the intervention of the Court is now necessary to provide direction to the lower courts, and to law enforcement, to protect the rights to privacy and free speech, and to assure the uniformity of lower court decisions under the terms of the law.

CONCLUSION

For the reasons set forth above, and in light of the confusion which has plagued law enforcement and the courts in the interpretation of the Electronic Communications Privacy Act, the Petition for a Writ of Certiorari should be granted.

Respectfully submitted,

ROBERT C. KONOP
Petitioner Pro Se
8601 Falmouth #406
Playa del Rey, CA 90293
Phone: (310) 305-2837

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ROBERT C. KONOP, *Plaintiff-Appellant*, v. HAWAIIAN AIRLINES, INC., *Defendant-Appellee*.	No. 99-55106 D.C. No. CV-96-04898-SJL (JGx) OPINION

Appeal from the United States District Court
for the Central District of California
J. Spencer Letts, District Judge, Presiding

Argued and Submitted
June 8, 2000 – Pasadena, California

Opinion Filed January 8, 2001
Opinion Withdrawn August 28, 2001

Filed August 23, 2002

Before: Robert Boochever, Stephen Reinhardt, and Richard A. Paez, Circuit Judges.

Opinion by Judge Boochever;
Partial Concurrence and
Partial Dissent by Judge Reinhardt

COUNSEL

Robert C. Konop, Pro se, Playa del Rey, California, plaintiff-appellant.

Marianne Shipp, Gibson, Dunn & Crutcher, Irvine, California, for the defendant-appellee.

OPINION

BOOCHEVER, Circuit Judge:

Robert Konop brought suit against his employer, Hawaiian Airlines, Inc. ("Hawaiian"), alleging that Hawaiian viewed Konop's secure website without authorization, disclosed the contents of that website, and took other related actions in violation of the federal Wiretap Act, the Stored Communications Act, and the Railway Labor Act. Konop also alleged several state tort claims. The district court granted summary judgment against Konop on all claims, except his retaliation claim under the Railway Labor Act. On the retaliation claim, the district court entered judgment against Konop following a bench trial. Konop appeals the district court's judgement on all claims, except on those brought under state tort law.

On January 8, 2001, we issued an opinion, reversing the district court's decision on Konop's claims under the Wiretap Act and the Stored Communications Act, and on several of his claims under the Railway Labor Act. *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001). Hawaiian filed a petition for rehearing, which became moot when we withdrew our previous opinion. *Konop v. Hawaiian Airlines, Inc.*, 262 F.3d 972 (9th Cir. 2001). We now affirm the judgment of the district court with respect to Konop's Wiretap Act claims and his retaliation claim under the Railway Labor Act. We reverse the district court's judgment with respect to Konop's claims under the Stored Communications Act and his remaining claims under the Railway Labor Act.

FACTS

Konop, a pilot for Hawaiian, created and maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent union, Air Line Pilots Association ("ALPA"). Many of those criticisms related to Konop's opposition to labor concessions which Hawaiian sought from ALPA. Because ALPA supported the concessions, Konop, via his website, encouraged Hawaiian employees to consider alternative union representation.

Konop controlled access to his website by requiring visitors to log in with a user name and password. He created a list of people, mostly pilots and other employees of Hawaiian, who were eligible to access the website. Pilots Gene Wong and James Gardner were included on this list. Konop programmed the website to allow access when a person entered the name of an eligible person, created a password, and clicked the "SUBMIT" button on the screen, indicating acceptance of the terms and conditions of use. These terms and conditions prohibited any member of Hawaiian's management from viewing the website and prohibited users from disclosing the website's contents to anyone else.

In December 1995, Hawaiian vice president James Davis asked Wong for permission to use Wong's name to access Konop's website. Wong agreed. Davis claimed he was concerned about untruthful allegations that he believed Konop was making on the website. Wong had not previously logged into the website to create an account. When Davis accessed the website using Wong's name, he presumably typed in Wong's name, created a password, and clicked the "SUBMIT" button indicating acceptance of the terms and conditions.

Later that day, Konop received a call from the union chairman of ALPA, Reno Morella.[1] Morella told Konop that Hawaiian president Bruce Nobles had contacted him regarding the contents of Konop's website. Morella related that Nobles was upset by Konop's accusations that Nobles was suspected of fraud and by other disparaging statements published on the website. From this conversation with Morella, Konop believed Nobles had obtained the contents of his website and was threatening to sue Konop for defamation based on statements contained on the website.

After speaking with Morella, Konop took his website offline for the remainder of the day. He placed it back online the next morning, however, without knowing how Nobles had obtained the information discussed in the phone call. Konop claims to have learned only later from the examination of system logs that Davis had accessed the website using Wong's name.

In the meantime, Davis continued to view the website using Wong's name. Later, Davis also logged in with the name of another pilot, Gardner, who had similarly consented to Davis' use of his name. Through April 1996, Konop claims that his records indicate that Davis logged in over twenty times as Wong, and that Gardner or Davis logged in at least fourteen more times as Gardner.

Konop filed suit alleging claims under the federal Wiretap Act, the Stored Communications Act, the Railway

---

[1] The parties dispute the date and substance of this phone conversation. Because the district court granted summary judgment, we view the facts in the light most favorable to Konop.

Labor Act, and state tort law, arising from Davis' viewing and use of Konop's secure website. Konop also alleged that Hawaiian placed him on medical suspension in retaliation for his opposition to the proposed labor concessions, in violation of the Railway Labor Act. The district court granted summary judgment to Hawaiian on all but the retaliatory suspension claim, and entered judgment against Konop on that claim after a short bench trial.

Konop appeals, arguing that the district court erred in granting summary judgment to Hawaiian on his federal claims under the Wiretap Act, Stored Communications Act, and Railway Labor Act. In addition, Konop urges us to reverse the district court's judgment on the retaliation claim following the bench trial, because he claims the district court improperly quashed subpoenas for witnesses Konop sought to have testify at trial.

DISCUSSION

The district court's grant of summary judgment is reviewed de novo. *Lopez v. Smith,* 203 F.3d 1122, 1131 (9th Cir. 2000) (en banc). Viewing the evidence in the light most favorable to Konop, we must determine whether there are any genuine issues of material fact and whether the district court correctly applied the relevant substantive law. *Id.*

I. Electronic Communications Privacy Act Claims

We first turn to the difficult task of determining whether Hawaiian violated either the Wiretap Act, 18

U.S.C. §§ 2510-2522 (2000) or the Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2000),[2] when Davis accessed Konop's secure website. In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, which was intended to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to "address[ ] the interception of . . . electronic communications." S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. Title II of the ECPA created the Stored Communications Act (SCA), which was designed to "address[ ] access to stored wire and electronic communications and transactional records." *Id.*

As we have previously observed, the intersection of these two statutes "is a complex, often convoluted, area of the law." *United States v. Smith,* 155 F.3d 1051, 1055 (9th Cir. 1998). In the present case, the difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. *See. e.g.,* Robert A. Pikowsky, *Legal and Technological Issues Surrounding Privacy of Attorney Client Communication*

---

[2] The Wiretap Act and SCA have since been amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (October 26, 2001).

Via Email, Advocate, Oct. 2000, at 17-19 (discussing the uncertainty over email privacy caused by the ECPA and judicial interpretations thereof); Lieutenant Colonel LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See,* 46 A.F. L. Rev. 155, 171-74 (1999) (same); Tatsuya Akamine, Note, *Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act,* 7 J.L. Pol'y 519, 521-29, 561-68 (1999) (criticizing the judiciary's interpretation of the ECPA). We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain a confusing and uncertain area of the law.

A. The Internet and Secure Websites

The Internet is an international network of interconnected computers that allows millions of people to communicate and exchange information. *See Reno v. ACLU,* 521 U.S. 844, 849-50 (1997); *In re DoubleClick Inc. Privacy Litig.,* 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001). The World Wide Web, the best known category of communication over the Internet, consists of a vast number of electronic documents stored in different computers all over the world. *Reno v. ACLU,* 521 U.S. at 852. Any person or organization with a computer connected to the Internet can "publish" information on the Web in the form of a "web page" or "website." *See id.* at 853 & n.9. A website consists of electronic information stored by a hosting service computer or "server." The owner of the website may pay a fee for this service. Each website has a unique domain name or web address (*e.g.,* Amazon.com or Lycos.com), which corresponds to a specific location within

the server where the electronic information comprising the website is stored. A person who wishes to view the website types the domain name into a computer connected to the Internet. This is essentially a request to the server to make an electronic copy of the website (or at least the first page or "home page") and send it to the user's computer. After this electronic information reaches the user's computer, it is downloaded for viewing on the user's screen. *See generally* Preston Gralla, *How the Internet Works* (1999).

While most websites are public, many, such as Konop's, are restricted. For instance, some websites are password-protected, require a social security number, or require the user to purchase access by entering a credit card number. *See Reno,* 521 U.S. at 852-53, 856. The legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards. *See* S. Rep. No. 99-541, at 35-36 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public."); H.R. Rep. No. 99-647 at 41, 62-63 (1986) (describing the Committee's understanding that the configuration of the electronic communications system would determine whether or not an electronic communication was readily accessible to the public). The nature of the Internet, however, is such that if a user enters the appropriate information (password, social security number, etc.), it is nearly impossible to verify the true identity of that user. *Cf. Reno,* 521 U.S. at 855-56 (discussing the difficulty of verifying the age of a website user by requiring a credit card number or password).

We are confronted with such a situation here. Although Konop took certain steps to restrict the access of Davis and other managers to the website,[3] Davis was

---

[3] Specifically, Konop configured the website to allow access when a person typed in the correct web address, received the home page of his website, entered the name of an eligible person, created a password, and clicked the "SUBMIT" button indicating acceptance of the terms and conditions of use. In addition, Konop displayed the following language on the home page of his website:

> This is the gateway for NEWS UPDATES and EDITORIAL COMMENTS directed only toward Hawaiian Air's pilots and other employees, not including HAL management. By entering, you acknowledge and agree to the terms and conditions of use as specified below. You must read this entire page before entry. Others should simply find *something else* to do with their time.
>
> If you are already a registered user, you may fill in your name along with the other information required below, then enter the system. If you want to visit the system, and you belong to the authorized group, you must supply the proper information before you will be allowed to enter. Make note of the password you enter for your first visit, otherwise future visits may be delayed. Visits by others will be strictly prohibited.

Beneath this language, Konop provided boxes for a person's name, occupation, email address and password. Below the boxes were two buttons: one said "SUBMIT," the other said "CLEAR." The advisement continued:

> All name and contact information will be kept strictly confidential. Any effort to defeat, compromise or violate the security of this website will be prosecuted to the fullest extent of the law.
>
> WARNING!
>
> The information contained herein is CONFIDENTIAL, and it is not intended for public dissemination! By requesting entry in the system, you must agree not to furnish any of the information contained herein to any other person or for any other use. Republication or redistribution of this

(Continued on following page)

nevertheless able to access the website by entering the correct information, which was freely provided to Davis by individuals who were eligible to view the website.

B. Wiretap Act

Konop argues that Davis' conduct constitutes an interception of an electronic communication in violation of the Wiretap Act. The Wiretap Act makes it an offense to "intentionally intercept[ ] . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). We must therefore determine whether Konop's website is an "electronic communication" and, if so, whether Davis "intercepted" that communication.

An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." *Id.* § 2510(12). As discussed above, website owners such as Konop transmit electronic documents to servers, where the documents are stored. If a user wishes to view the website, the user requests that the server transmit a copy of the document to the user's computer. When the server sends the document to the user's computer for viewing, a transfer of information from the website owner to the user has occurred. Although the

---

information to any other person is strictly prohibited. Anyone found to disseminate this information to anyone other than those specifically named and allowed here will be banned from this website and held liable to prosecution for violation of the terms and conditions of use and for violation of this contract.

website owner's document does not go directly or immediately to the user, once a user accesses a website, information is transferred from the website owner to the user via one of the specified mediums. We therefore conclude that Konop's website fits the definition of "electronic communication."

The Wiretap Act, however, prohibits only "interceptions" of electronic communications. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). Standing alone, this definition would seem to suggest that an individual "intercepts" an electronic communication merely by "acquiring" its contents, regardless of when or under what circumstances the acquisition occurs. Courts, however, have clarified that Congress intended a narrower definition of "intercept" with regard to electronic communications.

In *Steve Jackson Games, Inc. v. United States Secret Service,* 36 F.3d 457 (5th Cir. 1994), the Fifth Circuit held that the government's acquisition of email messages stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, was not an "interception" under the Wiretap Act. The court observed that, prior to the enactment of the ECPA, the word "intercept" had been interpreted to mean the acquisition of a communication contemporaneous with transmission. *Id.* at 460 (*citing United States v. Turk,* 526 F.2d 654, 658 (5th Cir. 1976)). The court further observed that Congress, in passing the ECPA, intended to retain the previous definition of

"intercept" with respect to wire and oral communications,[4] while amending the Wiretap Act to cover interceptions of electronic communications. *See Steve Jackson Games*, 36 F.3d at 462; S. Rep. No. 99-541, at 13; H.R. Rep. No. 99-647, at 34. The court reasoned, however, that the word "intercept" could not describe the exact same conduct with respect to wire and electronic communications, because wire and electronic communications were defined differently in the statute. Specifically, the term "wire communication" was defined to include storage of the communication, while "electronic communication" was not.[5] The court concluded that this textual difference evidenced Congress' understanding that, although one could "intercept" a *wire* communication in storage, one could not "intercept" an *electronic* communication in storage:

> Critical to the issue before us is the fact that, unlike the definition of "wire communication," the definition of "electronic communication" does not include electronic storage of such communications. . . . Congress' use of the word "transfer" in the definition of "electronic communication," and its omission in that definition of the phrase "any electronic storage of such communication"

---

[4] Congress revised the definition of "intercept" slightly to clarify that non-voice portions of wire communications are also protected. *See* H.R. Rep. No. 99-647, at 34.

[5] Until October 2001, "wire communication" was defined as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception . . . and *such term includes any electronic storage of such communication*. . . ." 18 U.S.C. § 2510(1) (2000) (emphasis added).

> . . . reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage."

Steve Jackson Games, 36 F.3d at 461-62; *Wesley Coll. v. Pitts,* 974 F. Supp. 375, 386 (D. Del. 1997) ("[B]y including the electronic storage of wire communications within the definition of such communications but declining to do the same for electronic communications . . . Congress sufficiently evinced its intent to make acquisitions of electronic communications unlawful under the Wiretap Act only if they occur contemporaneously with their transmissions."), *aff'd,* 172 F.3d 861 (3d Cir. 1998); *United States v. Reyes,* 922 F. Supp. 818, 836 (S.D.N.Y. 1996) ("Taken together, the definitions thus imply a requirement that the acquisition of [electronic communications] be simultaneous with the original transmission of the data."); *Bohach v. City of Reno,* 932 F. Supp. 1232, 1236-37 (D. Nev. 1996) (requiring acquisition during transmission). The *Steve Jackson* Court further noted that the ECPA was deliberately structured to afford electronic communications *in storage* less protection than other forms of communication. *See Steve Jackson Games,* 36 F.3d at 462-64.

The Ninth Circuit endorsed the reasoning of *Steve Jackson Games* in *United States v. Smith,* 155 F.3d at 1051. The question presented in *Smith* was whether the Wiretap Act covered wire communications in storage, such as voice mail messages, or just wire communications in transmission, such as ongoing telephone conversations. Relying on the same textual distinction as the Fifth Circuit in *Steve Jackson Games,* we concluded that wire communications in storage could be "intercepted" under the Wiretap Act. We found that Congress' inclusion of

storage in the definition of "wire communication" militated in favor of a broad definition of the term "intercept" with respect to wire communications, one that included acquisition of a communication subsequent to transmission. We further observed that, *with respect to wire communications only,* the prior definition of "intercept" – acquisition contemporaneous with transmission – had been overruled by the ECPA. *Smith,* 155 F.3d at 1057 n.11. On the other hand, we suggested that the narrower definition of "intercept" was still appropriate with regard to electronic communications:

> [I]n cases concerning "electronic communications" – the definition of which specifically includes "transfers" and specifically excludes "storage" – the "narrow" definition of "intercept" fits like a glove; it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act. In fact, a number of courts adopting the narrow interpretation of "interception" have specifically premised their decisions to do so on the distinction between § 2510's definitions of wire and electronic communications.

Smith, 155 F.3d at 1057 (citations and alterations omitted).

We agree with the *Steve Jackson* and *Smith* courts that the narrow definition of "intercept" applies to electronic communications. Notably, Congress has since amended the Wiretap Act to eliminate storage from the definition of wire communication, *see* USA PATRIOT Act § 209, 115 Stat. at 283, such that the textual distinction relied upon by the *Steve Jackson* and *Smith* courts no longer exists. This change, however, supports the analysis of those cases. By eliminating storage from the definition

of wire communication, Congress essentially reinstated the pre-ECPA definition of "intercept" – acquisition contemporaneous with transmission – with respect to wire communications. *See Smith,* 155 F.3d at 1057 n.11. The purpose of the recent amendment was to reduce protection of voice mail messages to the lower level of protection provided other electronically stored communications. *See* H.R. Rep. 107-236(I), at 158-59 (2001). When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term "intercept" with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial definition of "intercept" as acquisition contemporaneous with transmission.

We therefore hold that for a website such as Konop's to be "intercepted" in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage.[6] This conclusion is consistent with the

---

[6] The dissent, amici, and several law review articles argue that the term "intercept" must apply to electronic communications in storage because storage is a necessary incident to the transmission of electronic communications. *See, e.g.,* Akamine, *supra,* at 561-65; Jarrod J. White, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail,* 48 Ala. L. Rev. 1079, 1083 (1997). Email and other electronic communications are stored at various junctures in various computers between the time the sender types the message and the recipient reads it. In addition, the transmission time of email is very short because it travels across the wires at the speed of light. It is therefore argued that if the term "intercept" does not apply to the *en route* storage of electronic communications, the Wiretap Act's prohibition against "intercepting" electronic communications would have virtually no effect. While this argument is not without appeal, the language and structure of the ECPA

(Continued on following page)

ordinary meaning of "intercept," which is "to stop, seize, or interrupt in progress or course before arrival." *Webster's Ninth New Collegiate Dictionary* 630 (1985). More importantly, it is consistent with the structure of the ECPA, which created the SCA for the express purpose of addressing "access to *stored* . . . electronic communications and transactional records." S. Rep. No. 99-541 at 3 (emphasis added). The level of protection provided stored communications under the SCA is considerably less than that provided communications covered by the Wiretap Act. Section 2703(a) of the SCA details the procedures law enforcement must follow to access the contents of stored electronic communications, but these procedures are considerably less burdensome and less restrictive than those required to obtain a wiretap order under the Wiretap Act. *See Steve Jackson Games,* 36 F.3d at 463. Thus, if Konop's position were correct and acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result. As the Fifth Circuit recognized in *Steve Jackson Games,* "it is most unlikely that Congress intended to require law

---

demonstrate that Congress considered and rejected this argument. Congress defined "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," 18 U.S.C. § 2510(17)(A), indicating that Congress understood that electronic storage was an inherent part of electronic communication. Nevertheless, as discussed above, Congress chose to afford stored electronic communications less protection than other forms of communication.

enforcement officers to satisfy the more stringent requirements for an intercept in order to gain access to the contents of stored electronic communications." *Id.; see also Wesley Coll.*, 974 F. Supp. at 388 (same).

Because we conclude that Davis' conduct did not constitute an "interception" of an electronic communication in violation of the Wiretap Act, we affirm the district court's grant of summary judgment against Konop on his Wiretap Act claims.[7]

C. Stored Communications Act

Konop also argues that, by viewing his secure website, Davis accessed a stored electronic communication without authorization in violation of the SCA. The SCA makes it an offense to "intentionally access[ ] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ ] . . . access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a)(1). The SCA excepts from liability, however, "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). The district court found that the exception in § 2701(c)(2) applied because Wong and Gardner consented to Davis' use of Konop's website. It therefore granted summary judgment to Hawaiian on the SCA claim.

---

[7] Konop also claims that Hawaiian violated the Wiretap Act when Davis used and disclosed the contents of Konop's website. As there was no interception under the Wiretap Act, this claim also fails.

The parties agree that the relevant "electronic communications service" is Konop's website, and that the website was in "electronic storage." In addition, for the purposes of this opinion, we accept the parties' assumption that Davis' conduct constituted "access without authorization"[8] to "a facility through which an electronic communication service is provided."

We therefore address only the narrow question of whether the district court properly found Hawaiian exempt from liability under § 2701(c)(2). Section 2701(c)(2) allows a person to authorize a third party's access to an electronic communication if the person is 1) a "user" of the "service" and 2) the communication is "of or intended for that user." *See* 18 U.S.C. § 2701(c)(2). A "user" is "any person or entity who – (A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13).

The district court concluded that Wong and Gardner had the authority under § 2701(c)(2) to consent to Davis' use of the website because Konop put Wong and Gardner on the list of eligible users. This conclusion is consistent

---

[8] The term "without authorization" is not defined in the statute. *Cf. EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581-82 & n.10 (1st Cir.2001) (explaining, with respect to alleged unauthorized use of a website, Congress' failure to define "without authorization" in the Computer Fraud and Abuse Act, and discussing some possible, practicable definitions of the term). There is some indication in the legislative history that Congress intended the configuration of the electronic communication system to "establish an objective standard [for] determining whether a system receives privacy protection." H.R. Rep. No. 99-647, at 41. Since the issue is not properly before us, however, we express no opinion on how the term "without authorization" should be defined with respect to a non-public website such as Konop's.

with other parts of the Wiretap Act and the SCA which allow intended recipients of wire and electronic communications to authorize third parties to access those communications.[9] In addition, there is some indication in the legislative history that Congress believed "addressees" or "intended recipients" of electronic communications would have the authority under the SCA to allow third parties access to those communications. *See* H.R. Rep. No. 99-647, at 66-67 (explaining that "an addressee [of an electronic communication] may consent to the disclosure of a communication to any other person" and that "[a] person may be an 'intended recipient' of a communication . . . even if he is not individually identified by name or otherwise").

Nevertheless, the plain language of § 2701(c)(2) indicates that only a "user" of the service can authorize a third party's access to the communication. The statute defines "user" as one who 1) *uses* the service and 2) is duly authorized to do so. Because the statutory language is unambiguous, it must control our construction of the statute, notwithstanding the legislative history. *See United States v. Daas,* 198 F.3d 1167, 1174 (9th Cir. 1999). The statute does not define the word "use," so we apply the ordinary definition, which is "to put into action or service, avail oneself of, employ." *Webster's* at 1299; *see Daas,* 198

[9] For instance, § 2702(b)(1) permits service providers to divulge the contents of stored communications "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." *See also id.* § 2702(b)(3) (providing a similar exception with respect to remote computing services). Similarly, the "consent" exception to the Wiretap Act allows one party to a wire communication to authorize a third party to intercept the communication. *See* 18 U.S.C. § 2511(2)(c) & (d).

F.3d at 1174 ("If the statute uses a term which it does not define, the court gives that term its ordinary meaning.").

Based on the common definition of the word "use," we cannot find any evidence in the record that Wong ever used Konop's website. There is some evidence, however, that Gardner may have used the website, but it is unclear when that use occurred. At any rate, the district court did not make any findings on whether Wong and Gardner actually used Konop's website – it simply assumed that Wong and Gardner, by virtue of being eligible to view the website, could authorize Davis' access. The problem with this approach is that it essentially reads the "user" requirement out of § 2701(c)(2). Taking the facts in the light most favorable to Konop, we must assume that neither Wong nor Gardner was a "user" of the website at the time he authorized Davis to view it. We therefore reverse the district court's grant of summary judgment to Hawaiian on Konop's SCA claim.

II. Railway Labor Act Claims

Konop also appeals the district court's grant of summary judgment to Hawaiian on his claims under the Railway Labor Act, 45 U.S.C. §§ 151-188 ("RLA"). The RLA prohibits "interference, influence, or coercion by either party over the designation of representatives by the other." 45 U.S.C. § 152 (Third). It also declares that "it shall be unlawful for any carrier to interfere in any way with the organization of its employees, or to use the funds of the carrier in maintaining or assisting or contributing to any labor organization, labor representative, or other agency of collective bargaining. . . . " *Id.* at § 152 (Fourth).

Konop asserts three claims under 45 U.S.C. § 152 (Third) and (Fourth) of the RLA. First, Konop alleges that Hawaiian interfered with his organizing efforts by accessing his website under false pretenses. Second, Konop alleges that Hawaiian wrongfully assisted a labor group by disclosing the contents of Konop's website to a union leader who supported the concessionary contract. Third, Konop alleges that Hawaiian engaged in coercion and intimidation by threatening to file a defamation suit against Konop based on statements on the website. The district court dismissed these claims on the alternative grounds that it lacked jurisdiction over the RLA claims, and that Konop failed to support them with evidence sufficient to withstand summary judgment.

A. Subject Matter Jurisdiction

Federal courts lack subject matter jurisdiction over disputes which are "grounded in the [collective bargaining agreement]," *Haw. Airlines, Inc. v. Norris,* 512 U.S. 246, 256 (1994), and "involve controversies over the meaning of an existing collective bargaining agreement in a particular fact situation," *id.* at 253 (internal quotation marks omitted). Such disputes, labeled "minor" disputes under the RLA, are subject to mandatory arbitration. *Id.* Hawaiian argues, and the district court agreed, that Konop's RLA claims are grounded in the collective bargaining agreement ("CBA") and are therefore subject to mandatory arbitration. We disagree.

In *Fennessy v. Southwest Airlines,* 91 F.3d 1359 (9th Cir. 1996), we addressed whether the district court had jurisdiction over the plaintiff's statutory claim under the RLA. The plaintiff in *Fennessy* alleged that the carrier

violated 45 U.S.C. § 152 (Fourth) by terminating his employment in retaliation for his efforts to replace the existing union. *Id.* at 1360-61. We held that "because his claim is based on a statutory provision rather than on the collective bargaining contract, it is not a minor dispute that must be brought to [arbitration]; it is a statutory claim that he may bring directly in district court." *Id.* at 1362. The plaintiff's unsuccessful arbitration of a related contractual claim under the CBA did not alter this conclusion. Because the statutory claims were not "grounded in the collective-bargaining agreement," and the statutory rights were "independent of the CBA," we found the district court had jurisdiction. *Id.*

Hawaiian argues that, unlike the statutory claim in *Fennessy,* Konop's statutory claims are grounded in and dependent on the CBA. To support this position, Hawaiian focuses on conduct which Konop explicitly alleged in his complaint as violating the CBA. Specifically, in the RLA section of the complaint, Konop alleged that Hawaiian violated the CBA by suspending him from work, reducing his employee benefits, requiring him to submit to physical and psychological testing, and giving certain pilots paid opportunities to campaign in favor of the concessionary contract.

On appeal, however, Konop does not challenge the district court's dismissal of these CBA-related claims. Rather, he objects to the district court's dismissal of his independent RLA claims. Konop claims that Hawaiian violated the RLA by (1) accessing his website under false pretenses, (2) disclosing the website's contents to the rival union faction, and (3) threatening to sue Konop for defamation based on statements on the website. Hawaiian never explains how these RLA claims are grounded in the

CBA, except to say that Konop merely presents them as a precursor to the alleged CBA violations. Nothing, however, requires such a narrow reading of Konop's allegations. Konop, like the plaintiff in *Fennessy,* presents his statutory claims as independent violations of the RLA. These claims in no way depend upon a finding that Hawaiian, at some later time, violated Konop's contractual rights under the CBA.

Accordingly, we hold that the RLA claims which Konop presses on appeal are not grounded in the CBA, are not subject to mandatory arbitration and, therefore, fall within the court's jurisdiction.

B. Protected Activity

Hawaiian contends that even if Hawaiian managers accessed Konop's website under false pretenses, conveyed this information to a rival union leader, and threatened to sue Konop for defamation, such conduct did not violate the RLA because it did not interfere with any protected organizing activity. The organizing activity in which Konop engaged principally involved the publication of articles on a secure website. As discussed above, Konop limited access to pilots and other employees on the eligible list and prohibited users from disclosing the contents of the website to others. He also categorically excluded managers. Konop's website publication vigorously criticized Hawaiian management and its proposal for wage concessions in the existing collective bargaining agreement. Because the incumbent union, ALPA, supported the concessionary contract, Konop sought to encourage consideration of alternative union representation.

There is no dispute that Konop's website publication would ordinarily constitute protected union organizing activity under the RLA. Hawaiian argues, however, that Konop forfeited any protection he would otherwise enjoy because his articles contained malicious, defamatory and insulting material known to be false. In *Linn v. United Plant Guard Workers, Local 114,* 383 U.S. 53, 61 (1966), the Supreme Court held that a party forfeits his protection under the National Labor Relations Act (NLRA) by "circulating defamatory or insulting material known to be false."[10] *See also Old Dominion Branch No. 496, Nat'l Ass'n of Letter Carriers v. Austin,* 418 U.S. 264, 282-83 (1974); *San Antonio Comm. Hosp. v. S. Cal. Dist. Council of Carpenters,* 125 F.3d 1230, 1237 (9th Cir. 1997).

We assume Hawaiian is referring to the alleged defamatory statements contained in the "Facts" section of its brief. There, Hawaiian indicates that Konop published the following false statements: (1) Nobles does his "dirty work . . . like the Nazis during World War II"; (2) "Soviet Negotiating Style Essential to Nobles Plan!"; (3) Nobles is "one incompetent at the top"; (4) Nobles "has little skill and little ability with people. . . . In fact, with as few skills as Nobles possesses, it is difficult to imagine how he got this far"; and (5) "Nobles Suspected in Fraud!" and "Hawaiian Air president, Bruce Nobles, is the prime suspect in an alleged fraud which took place in 1991."

---

[10] While employers covered under the RLA are not subject to the provisions of the NLRA, courts look to the NLRA and the cases interpreting it for guidance. *Bhd. of R.R. Trainmen v. Jacksonville Terminal Co.,* 394 U.S. 369, 383 (1969). We see no reason why the rule announced in *Linn,* 383 U.S. at 61, regarding protected activities, should not apply in the context of the RLA.

The first two statements, referencing the Nazis and Soviets, are simply "rhetorical hyperbole" protected by federal labor laws. *See Letter Carriers,* 418 U.S. at 286. The second two statements, commenting on Nobles' competence and people skills, are opinions also protected by federal labor laws. *See id.* at 284; *San Antonio Comm. Hosp.,* 125 F.3d at 1237. Konop did not forfeit his protection under the Railway Labor Act, as Hawaiian suggests, simply by publishing statements that were critical of and insulting to Nobles. " '[F]ederal law gives a union license to use intemperate, abusive, or *insulting* language without fear of restraint or penalty. . . . ' " *San Antonio Comm. Hosp.,* 125 F.3d at 1235 (quoting *Letter Carriers,* 418 U.S. at 283) (emphasis added); *see also Linn,* 383 U.S. at 58 ("[R]epresentation campaigns are frequently characterized by bitter and extreme charges, countercharges, unfounded rumors, vituperations, personal accusations, misrepresentations and distortions.").[11]

With respect to the final challenged statement, indicating that Nobles was suspected of fraud, Hawaiian fails to argue or present any evidence that Konop published the statement with knowledge of its falsity or with reckless disregard for the truth. Federal labor law protects even

---

[11] We recognize that some organizing activity may be "so flagrant, violent or extreme" or so "egregious," "opprobrious," "offensive," "obscene" or "wholly unjustified" that it loses the protection of the RLA. *See Reef Indus. v. NLRB,* 952 F.2d 830, 837 & n.19 (5th Cir. 1991) (per curiam); *Timekeeping Sys., Inc. & Lawrence Leinweber,* 323 N.L.R.B. 244, 248-50 (1997). It is not clear whether Hawaiian is contending that Konop's conduct falls within one of these more amorphous standards. Assuming Hawaiian does so contend, we nevertheless find Hawaiian has failed to demonstrate that, as a matter of law, Konop's activities were so intolerable as to lose their protection under the RLA.

false and defamatory statements unless such statements are made with actual malice – *i.e.,* knowledge of falsity or with reckless disregard for the truth. *See Letter Carriers,* 418 U.S. at 281; *Linn,* 383 U.S. at 61 (protection under labor law existed "even though the statements [were] erroneous and defame[d] one of the parties to the dispute"). With no evidence or argument that Konop acted with actual malice, Hawaiian cannot demonstrate as a matter of law that Konop forfeited his protection under the RLA.

NLRB v. Pincus Bros., Inc.-Maxwell, 620 F.2d 367 (3d Cir. 1980) (as amended), upon which Hawaiian principally relies, provides little support for Hawaiian's position. In *Pincus Bros.,* the Third Circuit, in considering whether the NLRB abused its discretion by declining to defer to an arbitration award, merely concluded it was "at least arguable" that the employee published a defamatory statement known to be false. *Id.* at 376. For Hawaiian to prevail on summary judgment, however, it must do more than show it is "at least arguable" that Konop knew the challenged statement was false. It must demonstrate this as a matter of law. As Hawaiian presents no evidence or argument that Konop acted with the requisite malice, Hawaiian falls short of satisfying this burden.

Accordingly, we find that Konop has raised a triable issue of fact with respect to whether the development and maintenance of his website constituted protected activity under the RLA.

C. Specific Violations

Konop argues that Hawaiian managers: (1) interfered with Konop's organizing efforts by viewing the website

under false pretenses, (2) wrongfully supported one labor group in favor of another by informing the opposing labor faction of the website's contents, and (3) engaged in coercion and intimidation by threatening to sue Konop for defamation, all in violation of the RLA. Hawaiian argues, and the district court agreed, that Konop failed to present sufficient evidence to withstand summary judgment on these claims. We disagree.

1. Access of Website

Konop argues that Davis interfered with Konop's organizing efforts by viewing the website under false pretenses. Absent a legitimate justification, employers are generally prohibited from engaging in surveillance of union organizing activities. *Cal. Acrylic Indus. v. NLRB,* 150 F.3d 1095, 1099-1100 (9th Cir. 1998). The reason for this general proscription is that employer surveillance "tends to create fear among employees of future reprisal" and, thus, "chills an employee's freedom to exercise" his rights under federal labor law. *Id.* at 1099.

In *NLRB v. Unbelievable, Inc.,* 71 F.3d 1434 (9th Cir. 1995), we upheld the Board's finding that the employer "engaged in unfair labor practices by eavesdropping on private conversations between employees and [a] Union representative," which occurred in the employee break room. *Id.* at 1438-39. We see no principled distinction between the employer's eavesdropping in *Unbelievable* and Hawaiian's access of Konop's secure website.

Hawaiian suggests that Davis had a legitimate reason to access Konop's website – to identify and correct any false or misleading statements. Assuming such a concern could justify Davis' monitoring of private union organizing

activities, Hawaiian has presented little evidence to suggest that any statements on Konop's website were actually defamatory. Moreover, as discussed below, there are triable issues whether Hawaiian used information it obtained from the website to assist one union faction over another, and to coerce and intimidate Konop. Under these circumstances, we conclude that Konop has raised a triable issue that Hawaiian's access of Konop's website was not justified.

Hawaiian also argues that Davis' access did not violate the RLA because it did not appreciably limit Konop's organizing activities. Hawaiian emphasizes that, after learning about Davis' access to the website, Konop restricted access for a mere half-day and declined to temper the language in his articles. Hawaiian, however, presents no authority indicating that employees subject to surveillance or eavesdropping must also demonstrate that they consequently limited their organizing activity. It is the *tendency* to chill protected activities, not the actual chilling of protected activities, that renders eavesdropping and surveillance generally objectionable under federal labor law. *See, e.g., Cal. Acrylic,* 150 F.3d at 1099-1100. That a hardy individual might continue his organizing activities undeterred, despite an employer's surveillance, does not render the employer's conduct any less of a violation.[12]

---

[12] Hawaiian also presents this argument to defeat the other two alleged RLA claims discussed in the following sections. We find it is no more persuasive in the context of those claims.

Accordingly, we find that Konop has raised a triable issue of fact that Hawaiian interfered with Konop's union organizing activity in violation of the RLA by accessing Konop's website.

2. Disclosure to Opposing Union

Konop argues that Nobles unlawfully assisted Reno Morella, the union leader who supported the concessionary contract, by disclosing the contents of Konop's website. Generally, the RLA prohibits employers from providing assistance to a union or labor faction. *See Barthelemy v. Air Lines Pilots Ass'n,* 897 F.2d 999, 1009 (9th Cir. 1990) (per curiam); *see also NLRB v. Finishline Indus.,* 451 F.2d 1280, 1281-82 (9th Cir. 1971) (NLRA prohibits employer from telling workers to withdraw from one union and join another); *NLRB v. L. Ronney & Sons Furniture Mfg. Co.,* 206 F.2d 730, 734-35 (9th Cir. 1953) (NLRA prohibits employer from initiating membership drive among his employees for employer-favored union).

Konop argues that Nobles disclosed useful intelligence to a rival union faction in an effort to ensure that Konop's faction, which opposed the concessionary contract, would not prevail. Hawaiian does not seriously dispute that disclosure of the contents of Konop's website to Morella would constitute improper assistance. Instead, Hawaiian argues that Konop failed to present sufficient evidence that Nobles made any such disclosure or that Nobles was even familiar with the contents of Konop's website when he spoke to Morella.

Morella, however, states in his declaration that Nobles contacted him on December 14, 1995 and informed him "that he had just reviewed information which was posted

on an internet communications system operated by Hawaiian Airlines Pilot Robert Konop." In addition, Morella states that Nobles also "disclosed to me that Konop's internet communications system contained a third written article concerning Konop's efforts to obtain union representation by a labor organization other than the Air Line Pilots Association." This evidence creates a genuine issue of fact whether Nobles was familiar with the contents of Konop's website and whether Nobles disclosed the contents of the website to Morella.

Moreover, Nobles confirmed in his declaration that he contacted Morella because he "felt that Reno Morella, the Chairman of the ALPA Master Executive Council, should be aware of the newsletter because of its inaccurate attack on the proposed labor agreements and the unfair effect it could have on the ratification process." Nobles thus effectively concedes that he interceded to help ensure that Morella's faction – which favored ratification of the concessionary contract – would prevail over Konop's faction, which opposed the agreement.

Accordingly, we find that Konop has raised a triable issue of fact whether Nobles improperly assisted one union faction over another in violation of the RLA.

3. Threat of Defamation Suit

Konop argues that Nobles engaged in unlawful coercion and intimidation by threatening to file a defamation suit against Konop based on statements on Konop's website. An employer's filing or threatened filing of a lawsuit against an employee concerning union organizing activities may, under certain circumstances, violate the RLA. *See, e.g., Diamond Walnut Growers, Inc. v. NLRB,* 53

F.3d 1085, 1089-90 (9th Cir. 1995) (finding employer's defamation lawsuit against union violated NLRA); *GHR Energy Corp.,* 294 N.L.R.B. 1011, 1014 (1989) (analyzing whether employer's threat to sue employee for defamation violated NLRA), *aff'd,* 924 F.2d 1055 (5th Cir. 1991).

Hawaiian does not argue that Nobles would be justified in threatening to sue Konop for defamation. Instead, Hawaiian contends that Konop failed to present sufficient evidence that Nobles ever made such a threat. Nobles stated in his declaration that he "did mention to Morella that the gross inaccuracies and lies in the newsletter made by Konop amounted to defamation," but that he "never said that [he] intended to file a lawsuit against Konop."

Morella, however, indicates otherwise. Morella states in his declaration, "Nobles advised me that Konop should be cautioned, or informed, of the possibility of a defamation lawsuit by Nobles." Morella also testified, "[I]t was my impression and conclusion that Nobles intended for me to contact Konop, or take other action, for the purpose of opposing Konop's efforts to seek alternative union representation." Morella then "informed Konop of Mr. Nobles' statements . . . regarding caution with respect to a possible lawsuit against Konop for defamation." Konop confirms the same in his declaration. This evidence is sufficient to raise a triable issue of fact whether Nobles threatened to sue Konop for defamation.

Accordingly, we find that Konop has raised a triable issue of fact whether Nobles engaged in coercion and intimidation in violation of the RLA by threatening to sue Konop for defamation.

D. Bench Trial on Retaliation Claim

Konop's retaliation claim under the RLA was tried to the district court. The district court entered judgment against him on this claim, which involved his allegation that Hawaiian violated the RLA when it placed him on sick leave in retaliation for protected labor activities. Konop challenges the district court's judgment on this claim on the ground that his subpoenas for corroborating witnesses were improperly quashed. We review a district court's order quashing subpoenas for an abuse of discretion. *United States v. Berberian,* 767 F.2d 1324, 1324 (9th Cir. 1985). A litigant whose subpoenas have been improperly quashed must also show prejudice. *See Casino Foods Corp. v. Kraftco Corp.,* 546 F.2d 301, 302 (9th Cir. 1976).

There is some dispute whether the district court's remarks in a pretrial hearing constituted an order to quash subpoenas at all. Assuming, however, that the district court did quash Konop's subpoenas, Konop has not suggested what relevant evidence the subpoenaed witnesses might have provided had they been compelled to testify. Konop has consequently failed to show that he was prejudiced. Accordingly, the district court's judgment against Konop on his retaliation claim under the RLA is affirmed.

CONCLUSION

For the foregoing reasons, we affirm the district court's judgment with respect to Konop's Wiretap Act claims and his retaliation claim under the Railway Labor Act. We reverse the district court's judgment on Konop's Stored Communications Act claims and his claims under the Railway Labor Act for interference with organizing

activities, wrongful support of a union faction, and coercion and intimidation.

AFFIRMED IN PART, REVERSED IN PART, and REMANDED.

REINHARDT, Circuit Judge, concurring in part, dissenting in part.

I concur in Part C of Section I of the majority opinion regarding Konop's claims under the Stored Communications Act, and Section II of the majority opinion regarding Konop's claims under the Railway Labor Act. I dissent, however, from Part B of Section I, which holds that the term "intercept" in the Wiretap Act, as applied to electronic communications, refers solely to *contemporaneous* acquisition. I conclude instead that "stored electronic communications" are subject to the statute's intercept prohibition as well.

Because I recognize that any reading of the relevant statutory provisions raises some difficulties and introduces some inconsistencies, the question becomes: which reading is more coherent and more consistent with Congressional intent? The majority reasons, and I agree, that stored electronic communications are covered under the definition of "electronic communications" in the Wiretap Act. However, having made that determination, the majority proceeds to introduce unnecessary confusion and incoherence into the statute by holding that "intercept" encompasses only *contemporaneous* acquisition of electronic communications, and thus that it is not possible to "intercept" a stored electronic communication. We have already rejected just such a contemporaneity requirement with respect to the acquisition of stored wire communications,

and there is no justification for reviving it with respect to stored electronic communications. *United States v. Smith*, 155 F.3d 1051, 1057 n.11, 1058 (9th Cir. 1998).

The contemporaneity requirement for interception first appeared in *United States v. Turk*, 526 F.2d 654 (5th Cir. 1976), in which the Fifth Circuit held that the definition of "intercept" in the statute "require[s] participation by the one charged with an 'interception' in the *contemporaneous* acquisition of the communication through the use of [a] device." 526 F.2d at 658 (emphasis added). In *Turk*, however, the Fifth Circuit was interpreting a version of the Wiretap Act that predates the one at issue in *Smith* and in this case. That version did not cover interception of stored wire communications or of electronic communications at all. The statute was subsequently amended to include electronic communications, stored electronic communications, and stored wire communications in 1986.[1] Electronic Communications Privacy Act. Pub. L. No. 99-508. 100 Stat. 1848. Thereafter, in *Smith*, 155 F.3d 1051, 1057 n.11, 1058 (9th Cir. 1998), this court held, in a case involving the acquisition of stored voicemail messages, that *Turk's* contemporaneity requirement had been "statutorily overruled," at least with respect to wire communications, by the changes in the statute which

[1] The statute was again recently amended, this time to repeal the inclusion of stored wire communications in the definition of wire communication. Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283 (enacted October 26, 2001). However we apply here the version that was in effect at the time of the acts in question, Electronic Communications Privacy Act. Pub. L. No. 99-508. 100 Stat. 1848.

brought *stored* wire communications within its purview. The *Smith* court reasoned that "intercept" must necessarily include non-contemporaneous acquisition of stored wire communications because Congress had deliberately inserted stored wire communications into the intercept provision despite the fact that contemporaneous acquisition of stored wire communications is, by definition, impossible. 155 F.3d at 1058. To read "intercept" to include only contemporaneous acquisition would, of course, have rendered the intercept prohibition with respect to stored wire communications meaningless. *Id.*

Here, the majority's definition of "intercept" renders that prohibition meaningless with respect to stored electronic communications. The majority opinion would result in eliminating stored electronic communications from the purview of the intercept prohibition altogether, because a stored communication cannot be acquired contemporaneously with its transmission – it has already been transmitted. The majority's reading of the statute simply doesn't work: while explicitly holding that stored electronic communications are within the term "electronic communications" and that the intercept prohibition of the Wiretap Act applies to electronic communications, it also explicitly holds that interception of electronic communications is limited to contemporaneous acquisition, thereby *simultaneously* including and excluding stored electronic communications from the intercept prohibition.

To read a contemporaneity requirement into the definition of "intercept" renders the prohibition against the electronic communication interception largely superfluous, and violates the precept against interpreting one provision of a statute to negate another. *See e.g., Sorenson v. Secretary of the Treasury,* 475 U.S. 851 (1986) (applying

the whole act rule to the Omnibus Budget Reconciliation Act of 1981). Intercept of electronic communications is defined as any "acquisition of the contents of any . . . electronic . . . communication through the use of any . . . device." 18 U.S.C. § 2510(4). The nature of electronic communication is that it spends infinitesmal amounts of time "en route," unlike a phone call. Therefore, in order to "intercept" an electronic communication, one ordinarily obtains one of the copies made en route or at the destination. These copies constitute "stored electronic communications," as acknowledged by the majority. 18 U.S.C. § 2510(17)(A) ("'electronic storage' means . . . any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"). If intercept is defined as solely contemporaneous acquisition, then in contravention of Congressional intent, at most all acquisitions of the contents of electronic communications would escape the intercept prohibition entirely. Jarrod J. White, Commentary, E-Mail@Work.Com: Employer Monitoring of Employee E-Mail, 48 *Ala. L. Rev.* 1079, 1083 (1997) ("Following the Fifth Circuit's rationale, [and excluding stored electronic communications from the intercept prohibition] there is only a narrow window during which an E-mail interception may occur – the seconds or milliseconds before which a newly composed message is saved to any temporary location following a send command. Therefore, . . . [assuming that stored communications are excluded from the intercept prohibition], interception of E-mail within the prohibition of the ECPA is virtually impossible.").

The majority asserts that it is reasonable that the term "intercept" would describe different conduct with respect to wire communications than with respect to

electronic communications because different actions are required to intercept different kinds of communications. This reasoning fails because, although wire communications and electronic communications are quite different, stored wire communications are technologically equivalent to stored electronic communications. Thus it would make little sense to treat them differently. *See* 18 U.S.C. § 2510(1) (defining "wire communication" as including "any *electronic storage* of [wire] communication"). While Congress may not always act sensibly, there is no reason for the majority to presume that it failed to do so in this instance.

The Non-Contemporaneous Acquisition Reading Permits a Coherent Reading of the Wiretap Act and the Stored Communications Act Together, Consistent with Congressional Intent

Congress's clear intent, when amending the statute in 1986, was to regulate *access to* and *acquisition of* stored electronic communications. *See* S. Rep. No. 99-541 at 3-4 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557-8 (discussing Congressional intent to cover email and computerized recordkeeping systems). The majority's interpretation of the Wiretap Act depends in part on a tortured reading of the Stored Communications Act under which "access to" a communication is equated with "acquisition of" a communication, contrary to clear statutory language. Sections 2701 and 2703 of the Stored Communications Act regulate "access" to facilities where communications are stored and "access" to the communications themselves. The majority, relying on *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 463 (5th Cir. 1994) somehow reads these provisions as being analogous

to the "intercept" provisions of the Wiretap Act. 236 F.3d at 1044. However, "access" is more properly understood as being *qualitatively* different from "intercept," not *temporally* different, and as constituting a lesser included offense of "intercept." The "access" prohibitions in § 2701, in contrast to those regarding "interception" in § 2511, do not mention at all "acquisition" of the "contents" of any communication, but only "access," authorized and unauthorized, to them. "Access" is not defined in the statute, and therefore courts must apply the ordinary or technical meaning that the word has in the context of electronic communications. "Access" is defined in the Oxford English Dictionary as "[t]he habit or power of getting near or into contact with; entrance, admittance, admission (to the presence or use of) [noun]" and "[t]o gain access to (data, etc., held in a computer or computer-based system, or the system itself) [transitive verb]." As discussed above, "intercept" is defined in the statute as the actual acquisition of the contents of a communication. Given the plain language of the statute, the difference between the prohibition in 18 U.S.C. § 2511 ("intercept") and 18 U.S.C. § 2701 ("access") becomes more than semantic; it indicates that Congress intended that *only* 18 U.S.C. § 2511 prohibit the actual *acquisition* of the contents of a communication.

On the other hand, section 2703 (the structure of which the panel claims supports a "contemporaneous acquisition" reading of the text) sets out the parameters under which governmental authorities can gain "access" to the "contents" of stored electronic communications. That section provides that governmental authorities may obtain a search warrant to compel electronic communication service providers to disclose the contents of stored electronic communications. By its plain terms, it does not

provide a judicial means by which government authorities can *independently* intercept or acquire the contents of electronic communications. That is covered under 18 U.S.C. § 2516. Having excluded stored electronic communications from the Wiretap Act, the majority is forced to torture the statutory language of the Stored Communications Act in order to craft a reading of the statutes which accomplishes Congress's intent of establishing procedures by which governmental authorities may directly acquire the contents of stored electronic communications. A reading of the Wiretap Act which includes stored electronic communications under the intercept prohibition provides a plain answer – one that does not require linguistic gymnastics.

Furthermore, contrary to the arguments of Hawaiian Airlines and its amici, the drafting of a separate act specifically governing the contents of stored electronic communications (Stored Communications Act. 18 U.S.C. §§ 2702-03) was necessary, *even though* stored communications were included in the Wiretap Act. First, the damage caused by computer hackers (also known as "electronic trespassers") was a major concern of Congress in enacting the Electronic Communications Privacy Act and the Stored Communications Act. The separate provisions prohibiting unauthorized access were found necessary, in addition to the pre-existing prohibitions on interception, because computer hackers often do a great deal of damage to stored communications facilities and stored communications without ever acquiring the contents of those communications. *See United States v. Smith,* 155 F.3d 1051, 1058-59 (9th Cir. 1998) (explaining that the Stored Communications Act permits penalties against hackers who put themselves in the position to acquire a communication, but

the Wiretap Act penalizes those who go further and acquire the communication); *In re DoubleClick, Inc. Privacy Litigation*, No. 00 CIV 0641 NRB, 2001 WL 303744 at *7 (S.D.N.Y. 2001) (finding that Title II of ECPA was aimed at computer hackers); *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp.2d 817, 820 (E.D. Mich. 2000) (explaining that the general purpose of the ECPA was to create a cause of action against computer hackers.); *State Wide Photocopy, Corp. v. Tokai Financial Services, Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995) ("[T]he ECPA was primarily designed to provide a cause of action against computer hackers. . . . "). Hackers often use their unauthorized access to disrupt or prevent authorized access of others to stored communications facilities. *See* 18 U.S.C. § 2701 (prohibiting obtaining, altering or preventing access to wire or electronic communications without authorization). Moreover, the activities of hackers, and the mere potential that they could acquire the contents of electronic or wire communications in storage, create an atmosphere of anxiety in which computer users do not feel confident about the confidentiality of their communications, and productivity is hampered. These were all major concerns of Congress in enacting the Stored Communications Act, concerns which necessitated the drafting of a separate act even though stored electronic communications were already included under the definition of electronic communications.

Second, it is in the nature of electronic communication to be stored (both temporarily and permanently, as Congress indicated in the definition of electronic storage, 18 U.S.C. § 2510(17)), and it is in the nature of the electronic communications industry that electronic communications service providers (defined in 18 U.S.C. § 2510(15)) have

possession and control over large amounts of stored electronic communications. Therefore, electronic communications service providers would be an obvious source for law enforcement authorities who seek to obtain the contents of electronic communications. Recognizing that compelling disclosure by these entities would be one means by which government authorities might seek to obtain the contents of communications, Congress added a section setting out the procedures for compelling such disclosure. Michael S. Leib, E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception, 34 *Harv. J. on Legis.* 393, 414 (1997). There is no analogous storage of wire communication by wire communication service providers (i.e., telephone companies, also included under 18 U.S.C. § 2510(15)) such that guidelines would be needed on how governmental authorities could compel disclosure of stored wire communications from them.

Third, the Stored Communications Act is necessary to police the unauthorized access to electronic and wire communications facilities that is a necessary antecedent to illegal interception of those communications in storage. Were Congress to prohibit only actual acquisition of the contents of communications in storage, law enforcement would be powerless to do anything about persons who gained unauthorized access in preparation for interception (i.e., the acquisition of the contents of communications) until such persons had actually accomplished their unlawful mission. Further, because acquisition of the contents of an electronic communication in storage, or a wire communication in electronic storage does not disturb the "original" copy of such communication, actual acquisition of

these communications is likely to be much more difficult to detect and prove than unauthorized access to a facility. Therefore it is helpful to law enforcement to have in its arsenal a separate provision governing access.

In sum, a reading of the Wiretap Act that includes stored electronic communications in the statute's "intercept" prohibition is consistent with the nature of the technology at issue, leaves no unexplained statutory gaps, and renders none of the myriad provisions of either the Wiretap Act or the Stored Communications Act superfluous. Under such a reading, the Wiretap Act would prohibit the interception of electronic communications, both stored and en route, and subject violators to serious penalties. It would permit law enforcement to intercept such communications using a court order as indicated in § 2516. (Whether or not it would preserve the use of other less savory techniques is a matter this court is not called upon to decide.) A court order can be obtained by state prosecutors in connection with any one of a number of enumerated crimes, and by any assistant United States attorney for the investigation of any federal felony. Wire communications are treated similarly with only minor exceptions (for example, authorization to intercept wire communications is only available for a finite, though extensive, list of federal crimes); this reading, consistent with Congressional intent as revealed in the legislative history of the statute, rejects the idea that stored electronic communications are afforded a lesser degree of protection from interception than stored wire communications.[2]

---

[2] In its interpretation of the term "intercept," the majority relies in part on legislative history from the USA Patriot Act. As the Supreme

(Continued on following page)

Prior Precedent on the Wiretap Act and the Stored Communications Act Does Not Preclude the Non-Contemporaneous Acquisition Reading

This is a case of first impression in this circuit, and there is no binding authority on the regulation of stored electronic communications. There are no Supreme Court cases interpreting the provisions of the Wiretap Act and the Stored Communications Act as they relate to electronic communications, and the court of appeals decisions, in our circuit and others, either do not deal with stored electronic communications, or are superseded by changes in law and technology, or both. *United States v. Turk* predates the addition of the electronic provisions and language to the statute, and therefore is of little relevance. 526 F.2d 654 (5th Cir. 1976). More important, its contemporaneity requirement was expressly repudiated in *United States v. Smith*. 155 F.3d 1051, 1057 n.11, 1058 (9th Cir. 1998) ("[T]o the extent that *Turk* stands for a definition of "intercept" that necessarily entails contemporaneity, it has . . . been statutorily overruled."). *Steve Jackson Games* is the only circuit court case that involves stored electronic communications. As discussed above, the Fifth Circuit's reasoning is flawed, as it fails to consider the difference between "access" 18 U.S.C. § 2701 and "intercept" 18

Court has cautioned, however, "'the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one.'" *Consumer Product Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 109, 117 (1980) (quoting *United States v. Price*, 361 U.S. 304, 313 (1960)). Such subsequent legislative history will "rarely override a *reasonable interpretation* of a statute that can be gleaned from its language and legislative history prior to its enactment." *Id.* at 118 n.13 (emphasis added).

U.S.C. § 2511 and erroneously conflates the terms, reading them both to refer to the acquisition of the contents of a communication. 36 F.3d at 463. Moreover, *Steve Jackson Games* is rendered somewhat obsolete by the growth of the Internet, a phenomenon that the judges deciding that case could not have meaningfully incorporated into their reading of the statute. In particular, it would have been impossible to anticipate the expectations of privacy that people would develop regarding the Internet, expectations that are crucial to interpreting the statutory scheme consistent with Congressional intent to protect privacy interests. The other cases cited by the majority are district court cases, not binding on this court; they also have little persuasive value because they rely on the flawed reasoning of *Steve Jackson Games* and on the contemporaneity requirement that this court has rejected. *See Wesley College v. Pitts,* 974 F. Supp. 375, 386 (D. Del. 1997), *aff'd,* 172 F.3d 861 (3d Cir. 1998) (affirmed by the Third Circuit in an unpublished disposition, which therefore has no precedential value); *United States v. Reyes,* 922 F. Supp. 818, 836 (S.D.N.Y. 1996); *Bohach v. City of Reno,* 932 F. Supp. 1232, 1236-37 (D. Nev. 1996). Although this court in *United States v. Smith* correctly recognized the access/intercept distinction, our opinion contained unfortunate dicta regarding electronic communications. 155 F.3d 1051 at 1057. Because the case involved wire, not electronic, communications, those statements are not binding upon us.

Conclusion

In conclusion, because I believe that reading the Wiretap Act to prohibit interception of "stored electronic communications" provides a more coherent construction of

the Act and is more consistent with the text of the statute as well as with the Congressional intent underlying both the Wiretap Act and the Stored Communications Act, I respectfully dissent from Part B of Section I of the majority opinion.

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ROBERT C. KONOP, Plaintiff-Appellant, v. HAWAIIAN AIRLINES, INC., Defendant-Appellee.	No. 99-55106 D.C. No. CV-96-04898-SJL(JGx) Central District of California, Los Angeles ORDER (Filed Oct. 04, 2002)

Before: BOOCHEVER, REINHARDT and PAEZ, Circuit Judges

Judges Boochever and Paez have voted to deny the petition for rehearing. Judge Reinhardt has voted to grant the petition for rehearing. Judges Reinhardt and Paez have voted to deny the petition for rehearing en banc and Judge Boochever so recommends.

The full court has been advised of the petition for rehearing en banc and no active judge has requested a vote on whether to rehear the matter en banc. Fed. R.App.P.35.

The petitions for rehearing and rehearing en banc are DENIED.

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited.

(1) Except as otherwise specifically provided in this chapter any person who –

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;

* * *

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

* * *

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

§ 2701. Unlawful access to stored communications.

(a) OFFENSE. – Except as provided in subsection (c) of this section whoever –

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

* * *

(c) EXCEPTIONS. – Subsection (a) of this section does not apply with respect to conduct authorized –

(1) by the person or entity providing a wire or electronic communication service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

§ 2703. Required disclosure of customer communications or records.

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or

electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

* * *